PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-352321

(43)Date of publication of application : 21.12.2001

(51)Int.Cl. H04L 9/08
G06F 12/14

(21)Application number : 2000-179695

(22)Date of filing : 15.06.2000

(71)Applicant : SONY CORP

(72)Inventor : ISHIGURO RYUJI
OSAWA YOSHITOMO
OISHI TAKEO
ASANO TOMOYUKI
MITSUZAWA ATSUSHI

(30)Priority

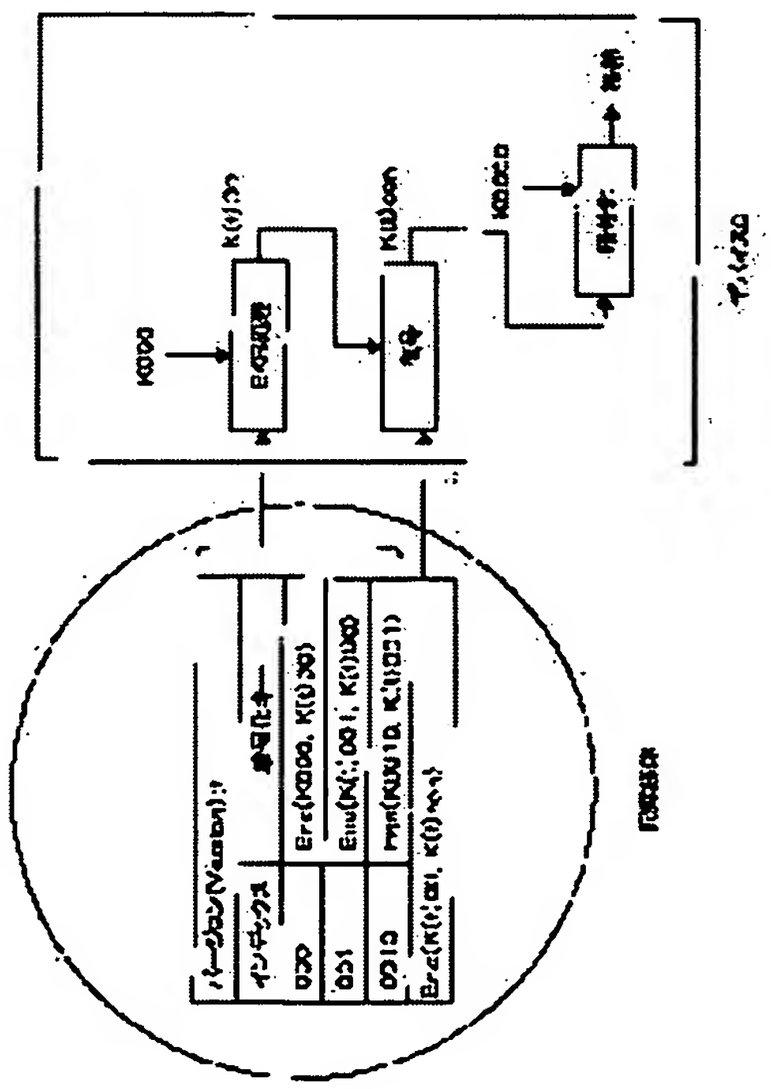
Priority number : 2000105329 Priority date : 06.04.2000 Priority country : JP

(54) INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize an information processing system and its method that execute distribution of various keys or data through an encryption key configuration adopting a tree structure so as to attain efficient and secure data distribution.

SOLUTION: A contents key, an authentication key, and program data or the like adopting an encryption key configuration employing a tree structure are transmitted with an effective key block(EKB). The EKB is configured to allow a device being a leaf of a tree to store a leaf key and a limited node key, and a specific effective key block (EKB) is generated for a group specified by a specific node and distributed thereto so as to limit devices that can be updated. Devices not belonging to the group



cannot be decoded and the distribution security of the keys or the like can be ensured.

LEGAL STATUS

[Date of request for examination]	26.11.2004
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－352321
（P2001－352321A）
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６０１Ａ　５Ｊ１０４
			６０１Ｄ

審査請求　未請求　請求項の数27　ＯＬ　（全 38 頁）

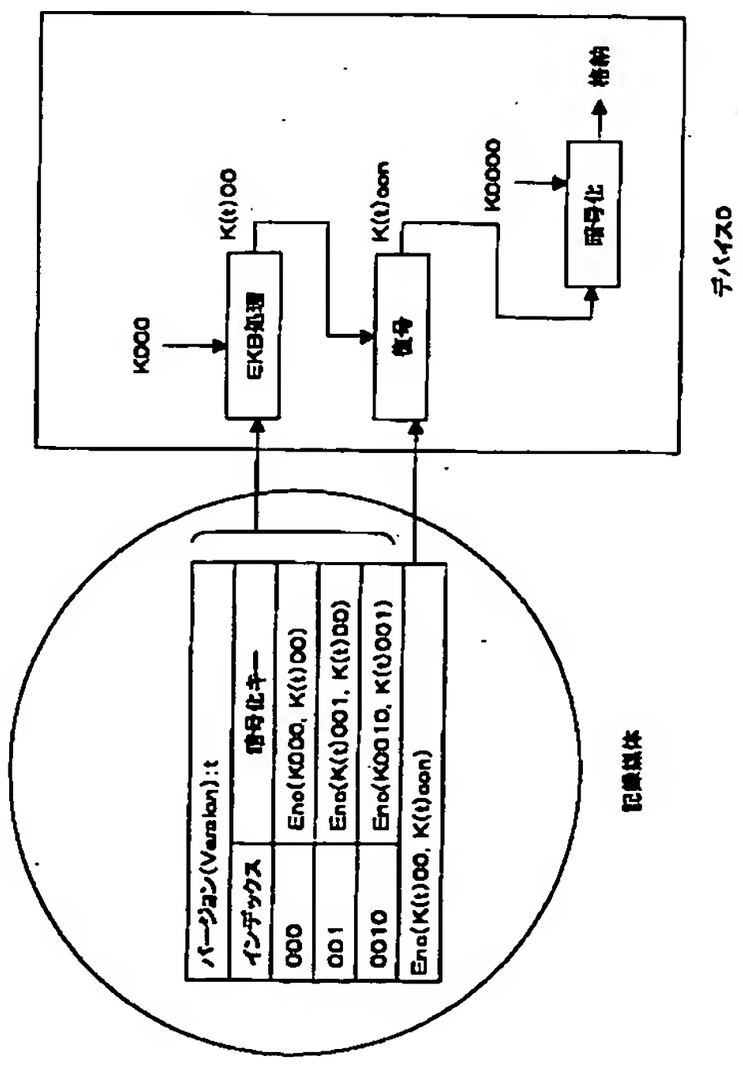
(21)出願番号　特願2000－179695(P2000－179695)
(22)出願日　平成12年６月15日(2000.6.15)
(31)優先権主張番号　特願2000－105329(P2000－105329)
(32)優先日　平成12年４月６日(2000.4.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】
【課題】　ツリー（木）構造の暗号化キー構成により各種キーまたはデータの配布を実行して、効率的、安全なデータ配信を可能とした情報処理システムおよび方法を実現する。
【解決手段】　ツリー構造の暗号化鍵構成により、コンテンツキー、認証キー、プログラムデータ等を有効化キーブロック（ＥＫＢ）とともに送信する。ＥＫＢは、ツリーのリーフを構成するデバイスにリーフキーおよび限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定の有効化キーブロック（ＥＫＢ）を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー等の配信安全性が確保される。



【特許請求の範囲】
【請求項１】１以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、
個々のデバイスは、
複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、
前記暗号化メッセージデータを配信するメッセージデータ配信手段は、
前記階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成して配信する構成を有することを特徴とする情報処理システム。
【請求項２】前記デバイスにおける前記暗号処理手段は、
前記有効化キーブロック（ＥＫＢ）の処理により、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求項１に記載の情報処理システム。
【請求項３】前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項１に記載の情報処理システム。
【請求項４】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項１に記載の情報処理システム。
【請求項５】前記メッセージデータは、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであることを特徴とする請求項１に記載の情報処理システム。
【請求項６】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項１に記載の情報処理システム。
【請求項７】前記メッセージデータは、プログラムコードであることを特徴とする請求項１に記載の情報処理システム。
【請求項８】前記メッセージデータ配信手段は、
前記有効化キーブロック（ＥＫＢ）と、
前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、
前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する構成であることを特徴とする請求項１に記載の情報処理システム。
【請求項９】前記メッセージデータ配信手段と前記デバイスは、
それぞれ認証処理を実行する認証処理手段を有し、
前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信する構成であることを特徴とする請求項１に記載の情報処理システム。
【請求項１０】前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、
前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）と暗号化メッセージデータを生成して配信する構成を有することを特徴とする請求項１に記載の情報処理システム。
【請求項１１】前記階層ツリー構造は、１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループによって構成されるカテゴリグループを含み、
該カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されていることを特徴とする請求項１に記載の情報処理システム。
【請求項１２】前記カテゴリグループは、さらに前記階層ツリー構造の下位段に１以上のサブカテゴリを含み、
該サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されていることを特徴とする請求項１１に記載の情報処理システム。
【請求項１３】１以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータをメッセージデータ配信手段から配信する情報処理方法であり、
複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、
前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップと、
を有することを特徴とする情報処理方法。
【請求項１４】前記復号処理ステップは、

前記有効化キーブロック（ＥＫＢ）の処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、
前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップと、
を含むことを特徴とする請求項１３に記載の情報処理方法。
【請求項１５】前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項１３に記載の情報処理方法。
【請求項１６】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項１３に記載の情報処理方法。
【請求項１７】前記メッセージデータは、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであることを特徴とする請求項１３に記載の情報処理方法。
【請求項１８】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項１３に記載の情報処理方法。
【請求項１９】前記メッセージデータは、プログラムコードであることを特徴とする請求項１３に記載の情報処理方法。
【請求項２０】前記メッセージデータ配信手段は、
前記有効化キーブロック（ＥＫＢ）と、
前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする請求項１３に記載の情報処理方法。
【請求項２１】前記メッセージデータ配信手段と前記デバイスは、
相互間の認証処理を実行し、
前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信することを特徴とする請求項１３に記載の情報処理方法。
【請求項２２】前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、
前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）と暗号化メッセージデータを生成して配信することを特徴とする請求項１３に記載の情報処理方法。
【請求項２３】データを格納した情報記録媒体であり、
複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）と、
前記更新ノードキーによって暗号化したメッセージデータと、
を格納したことを特徴とする情報記録媒体。
【請求項２４】前記メッセージデータはコンテンツの復号に用いるコンテンツキーであり、
前記情報記録媒体は、さらに、前記コンテンツキーによって暗号化された暗号化コンテンツを格納した構成であることを特徴とする請求項２３に記載の情報記録媒体。
【請求項２５】前記情報記録媒体は、さらに、
コンテンツと該コンテンツに対応するコンテンツキーを取得するために使用される有効化キーブロック（ＥＫＢ）を対応付けた対応付けデータを格納していることを特徴とする請求項２４に記載の情報記録媒体。
【請求項２６】前記情報記録媒体は、さらに、
コンテンツのインテグリティ・チェック値（ＩＣＶ）データを格納していることを特徴とする請求項２３に記載の情報記録媒体。
【請求項２７】暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、
前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、
前記コンテンツキーにより前記暗号化コンテンツの復号を実行するステップと、
を含むことを特徴とするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステムおよび方法に関する。特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、例えばコンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とする情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関する。
【０００２】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはＰＣ等のに付属する記録再生機器内の記録デバイス、例えばメモリカード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

【０００３】ビデオゲーム機器、ＰＣ等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはＤＶＤ、ＣＤ等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるＲＡＭ、ＲＯＭ等を有する。

【０００４】音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００５】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００６】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【０００７】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００８】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Deta encryption standard）がある。

【０００９】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【００１０】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【００１１】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはＤＶＤ、ＣＤ等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

【００１２】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行なう。認証方式

には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通な鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

【００１３】本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とする情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明の第１の側面は、１以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、前記暗号化メッセージデータを配信するメッセージデータ配信手段は、前記階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成して配信する構成を有することを特徴とする情報処理システムにある。

【００１５】さらに、本発明の情報処理システムの一実施態様において、前記デバイスにおける前記暗号処理手段は、前記有効化キーブロック（ＥＫＢ）の処理により、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする。

【００１６】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【００１７】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【００１８】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであることを特徴とする。

【００１９】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【００２０】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、プログラムコードであることを特徴とする。

【００２１】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段は、前記有効化キーブロック（ＥＫＢ）と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する構成であることを特徴とする。

【００２２】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段と前記デバイスは、それぞれ認証処理を実行する認証処理手段を有し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信する構成であることを特徴とする。

【００２３】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）と暗号化メッセージデータを生成して配信する構成を有することを特徴とする。

【００２４】さらに、本発明の情報処理システムの一実施態様において、前記階層ツリー構造は、１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループによって構成されるカテゴリグループを含み、該カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されていることを特徴とする。

【００２５】さらに、本発明の情報処理システムの一実施態様において、前記カテゴリグループは、さらに前記階層ツリー構造の下位段に１以上のサブカテゴリを含み、該サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されていることを特徴とする。

【００２６】さらに、本発明の第２の側面は、１以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータをメッセージデータ配信手段から配信する情報処理方法であり、複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくとも

いずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップと、を有することを特徴とする情報処理方法にある。

【００２７】さらに、本発明の情報処理方法の一実施態様において、前記復号処理ステップは、前記有効化キーブロック（ＥＫＢ）の処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含むことを特徴とする。

【００２８】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【００２９】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【００３０】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであることを特徴とする。

【００３１】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【００３２】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、プログラムコードであることを特徴とする。

【００３３】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータ配信手段は、前記有効化キーブロック（ＥＫＢ）と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする。

【００３４】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータ配信手段と前記デバイスは、相互間の認証処理を実行し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信することを特徴とする。

【００３５】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）と暗号化メッセージデータを生成して配信することを特徴とする。

【００３６】さらに、本発明の第３の側面は、データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）と、前記更新ノードキーによって暗号化したメッセージデータと、を格納したことを特徴とする情報記録媒体にある。

【００３７】さらに、本発明の情報記録媒体の一実施態様において、前記メッセージデータはコンテンツの復号に用いるコンテンツキーであり、前記情報記録媒体は、さらに、前記コンテンツキーによって暗号化された暗号化コンテンツを格納した構成であることを特徴とする。

【００３８】さらに、本発明の情報記録媒体の一実施態様において、コンテンツと該コンテンツに対応するコンテンツキーを取得するために使用される有効化キーブロック（ＥＫＢ）を対応付けた対応付けデータを格納していることを特徴とする。

【００３９】さらに、本発明の情報記録媒体の一実施態様において、コンテンツのインテグリティ・チェック値（ＩＣＶ）データを格納していることを特徴とする。

【００４０】さらに、本発明の第４の側面は、暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なるデバイスをリーフとした階層ツリー構造の１つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（ＥＫＢ）の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、前記コンテンツキーにより前記暗号化コンテンツの復号を実行するステップと、を含むことを特徴とするプログラム提供媒体にある。

【００４１】

【作用】本発明の構成においては、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キ

一更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの暗号鍵であるコンテンツキーもしくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キーブロックとともに配信する構成としている。

【００４２】このようにすることにより、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

【００４３】なお、本発明の第４の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００４４】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００４５】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４６】

【発明の実施の形態】［システム概要］図１に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側１０は、コンテンツ受信側２０の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側２０における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画像データ、音声データの再生、あるいは各種プログラムの実行等を行なう。コンテンツの配信側１０とコンテンツ受信側２０との間のデータ交換は、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体を介して実行される。

【００４７】コンテンツの配信側１０のデータ配信手段としては、インターネット１１、衛星放送１２、電話回線１３、ＤＶＤ、ＣＤ等のメディア１４等があり、一方、コンテンツ受信側２０のデバイスとしては、パーソナルコンピュータ（ＰＣ）２１、ポータブルデバイス（ＰＤ）２２、携帯電話、ＰＤＡ（Personal Digital Assistants）等の携帯機器２３、ＤＶＤ、ＣＤプレーヤ等の記録再生器２４、ゲーム端末等の再生専用器２５等がある。これらコンテンツ受信側２０の各デバイスは、コンテンツ配信側１０から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア３０から取得する。

【００４８】［デバイス構成］図２に、図１に示すコンテンツ受信側２０のデバイスの一例として、記録再生装置１００の構成ブロック図を示す。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ (Read Only Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０を有し、これらはバス１１０によって相互に接続されている。

【００４９】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００５０】暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００５１】ＲＯＭ１６０は、記録再生装置によって処理されるプログラムデータを格納する。ＣＰＵ１７０は、ＲＯＭ１６０、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログ

ラムや、ＣＰＵ１７０の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。

【００５２】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００５３】なお、図２に示す暗号処理手段１５０は、１つのワンチップＬＳＩとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

【００５４】［キー配信構成としてのツリー（木）構造について］次に、図１に示すコンテンツ配信側１０からコンテンツ受信側２０の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成およびデータ配信構成を図３を用いて説明する。

【００５５】図３の最下段に示すナンバ０～１５がコンテンツ受信側２０の個々のデバイスである。すなわち図３に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

【００５６】各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図３に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。図３の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【００５７】図３に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図３のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００５８】また、図３のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図３に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００５９】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【００６０】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【００６１】このツリー構造において、図３から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーＫｃｏｎをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号

Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を解いてコンテンツキー：Ｋｃｏｎを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【００６２】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【００６３】更新キーの配布処理ついて説明する。キーの更新は、例えば、図４（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図３に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：KeyRenewal Block）と呼ばれることもある。

【００６４】図４（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図４の例は、図３に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図３から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【００６５】図４（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図４（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイスＫ０００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイスＫ０００．Ｋ０００１は、図４（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを得ることができる。なお、図４（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００６６】図３に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図４（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００６７】図４（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキー：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）ｃｏｎ）を図４（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【００６８】すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【００６９】［ＥＫＢを使用したコンテンツキーの配布］図５に、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図４（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。すなわちＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００７０】図５に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。

【００７１】［ＥＫＢのフォーマット］図６に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン６０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ６０４はタグ部の位置、署名ポインタ６０５は署名の位置を示すポインタである。

【００７２】データ部６０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【００７３】タグ部６０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図７を用いて説明する。図７では、データとして先に図４（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図７の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図７の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図７（ｃ）に示すデータ列、およびタグ列が構成される。

【００７４】タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図４で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）

．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【００７５】図６に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【００７６】［ＥＫＢを使用したコンテンツキーおよびコンテンツの配信］上述の例では、コンテンツキーのみをＥＫＢとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、ＥＫＢによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

【００７７】図８にこのデータ構成を示す。図８（ａ）に示す構成において、Ｅｎｃ（Ｋｃｏｎ，ｃｏｎｔｅｎｔ）８０１は、コンテンツ（Content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータであり、Ｅｎｃ（ＫＥＫ，Ｋｃｏｎ）８０２は、コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ：Key Encryption Key）で暗号化したデータであり、Ｅｎｃ（ＥＫＢ，ＫＥＫ）８０３は、コンテンツキー暗号キーＫＥＫを有効化キーブロック（ＥＫＢ）によって暗号化したデータであることを示す。

【００７８】ここで、コンテンツキー暗号キーＫＥＫは、図３で示すノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（ＫＲ）自体であってもよく、またノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（ＫＲ）によって暗号化されたキーであってもよい。

【００７９】図８（ｂ）は、複数のコンテンツがメディアに記録され、それぞれが同じＥｎｃ（ＥＫＢ，ＫＥＫ）８０５を利用している場合の構成例を示す、このような構成においては、各データに同じＥｎｃ（ＥＫＢ，ＫＥＫ）を付加することなく、Ｅｎｃ（ＥＫＢ，ＫＥＫ）にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【００８０】図９にコンテンツキー暗号キーＫＥＫを、

図３に示すノードキーＫ００を更新した更新ノードキーＫ（ｔ）００として構成した場合の例を示す。この場合、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２に対して図９に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）で暗号化したデータと、（ｃ）コンテンツ（content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータとを配信することにより、デバイス０，１，２はコンテンツを得ることができる。

【００８１】図９の右側には、デバイス０における復号手順を示してある。デバイス０は、まず、受領した有効化キーブロックから自身の保有するリーフキーＫ０００を用いた復号処理により、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号によりコンテンツキーＫｃｏｎを取得し、さらにコンテンツキーＫｃｏｎによりコンテンツの復号を行なう。これらの処理により、デバイス０はコンテンツを利用可能となる。デバイス１，２においても各々異なる処理手順でＥＫＢを処理することにより、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【００８２】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【００８３】このように、ＥＫＢを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【００８４】なお、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツをＤＶＤ、ＣＤ等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック（ＥＫＢ）の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【００８５】図１０に記録媒体に暗号化コンテンツとともに有効化キーブロック（ＥＫＢ）を格納した構成例を示す。図１０に示す例においては、記録媒体にコンテンツＣ１～Ｃ４が格納され、さらに各格納コンテンツに対応するの有効化キーブロック（ＥＫＢ）を対応付けたデータが格納され、さらにバージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が格納されている。例えばＥＫＢ＿１はコンテンツＣ１を暗号化したコンテンツキーＫｃｏｎ１を生成するのに使用され、例えばＥＫＢ＿２はコンテンツＣ２を暗号化したコンテンツキーＫｃｏｎ２を生成するのに使用される。この例では、バージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が記録媒体に格納されており、コンテンツＣ３，Ｃ４は有効化キーブロック（ＥＫＢ＿Ｍ）に対応付けられているので、有効化キーブロック（ＥＫＢ＿Ｍ）の復号によりコンテンツＣ３，Ｃ４のコンテンツキーを取得することができる。ＥＫＢ＿１、ＥＫＢ＿２はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なＥＫＢ＿１，ＥＫＢ＿２を取得することが必要となる。

【００８６】図１１に、複数のデバイス間でコンテンツキーが流通する場合のＥＫＢを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。上段（ａ）従来構成であり、下段（ｂ）が本発明の有効化キーブロック（ＥＫＢ）を利用した例である。なお、図１１においてＫａ（Ｋｂ）は、ＫｂをＫａで暗号化したデータであることを示す。

【００８７】（ａ）に示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーＫｓｅｓを共有するために各デバイス間において、認証処理および鍵交換処理（ＡＫＥ：Authentication and Key Exchange）を実行し、認証が成立したことを条件としてセッションキーＫｓｅｓでコンテンツキーＫｃｏｎを暗号化して送信する処理を行なっていた。

【００８８】例えば図１１（ａ）のＰＣにおいては、受信したセッションキーで暗号化したコンテンツキーＫｓｅｓ（Ｋｃｏｎ）をセッションキーで復号してＫｃｏｎを得ることが可能であり、さらに取得したＫｃｏｎをＰＣ自体の保有する保存キーＫｓｔｒで暗号化して自身のメモリに保存することが可能となる。

【００８９】図１１（ａ）において、コンテンツプロバイダは、図１１（ａ）の記録デバイス１１０１にのみデータを利用可能な形で配信したい場合でも、間にＰＣ、再生装置が存在する場合は、図１１（ａ）に示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要とな

る。また、間に介在するＰＣ、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

【００９０】一方、図１１（ｂ）の下段に示す有効化キーブロック（ＥＫＢ）を利用した例においては、コンテンツプロバイダから有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）の処理によって得られるノードキー、またはルートキーによってコンテンツキーＫｃｏｎを暗号化したデータ（図の例ではＫｒｏｏｔ（Ｋｃｏｎ））を配信することにより、配信したＥＫＢの処理が可能な機器においてのみコンテンツキーＫｃｏｎを復号して取得することが可能になる。

【００９１】従って、例えば図１１（ｂ）の右端にのみ利用可能な有効化キーブロック（ＥＫＢ）を生成して、その有効化キーブロック（ＥＫＢ）と、そのＥＫＢ処理によって得られるノードキー、またはルートキーによってコンテンツキーＫｃｏｎを暗号化したデータを併せて送ることにより、間に存在するＰＣ、再生機器等は、自身の有するリーフキー、ノードキーによっては、ＥＫＢの処理を実行することができない。従って、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーＫｃｏｎの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

【００９２】ＰＣ、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キーブロック（ＥＫＢ）を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

【００９３】［有効化キーブロック（ＥＫＢ）を使用した認証キーの配信（共通鍵方式）］上述の有効化キーブロック（ＥＫＢ）を使用したデータあるいはキーの配信において、デバイス間で転送される有効化キーブロック（ＥＫＢ）およびコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝走路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理および鍵交換処理を実行することが有効な手段である。ここでは、この認証処理および鍵交換処理を実行する際に使用する認証キーＫａｋｅを上述の有効化キーブロック（ＥＫＢ）を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわちＥＫＢによる暗号化メッセージデータを認証キーとした例である。

【００９４】図１２に、共通鍵暗号方式を用いた相互認証方法（ISO/IEC 9798-2）を示す。図１２においては、共通鍵暗号方式としてＤＥＳを用いているが、共通鍵暗号方式であれば他の方式も可能である。図１２において、まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。なお、鍵Ｋａｂは、ＡおよびＢに共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。ＤＥＳのＣＢＣモードを用いた鍵Ｋａｂによる暗号化処理は、例えばＤＥＳを用いた処理においては、初期値とＲａとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ１を生成し、続けて暗号文Ｅ１とＲｂとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ２を生成し、さらに、暗号文Ｅ２とＩＤ（ｂ）とを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化して生成した暗号文Ｅ３とによって送信データ（Token-AB）を生成する。

【００９５】これを受信したＢは、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵Ｋａｂ（認証キー）で復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を認証キーＫａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を認証キーＫａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を認証キーＫａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)のうち、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【００９６】次にＢは、認証後に使用するセッションキー（Ｋｓｅｓ）を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで認証キーＫａｂを用いて暗号化し、Ａに返送する。

【００９７】これを受信したＡは、受信データを認証キーＫａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッションキーＫｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【００９８】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【００９９】上述の認証処理においては、Ａ，Ｂは共通

の認証キーＫａｂを共有する。この共通鍵Ｋａｂを上述の有効化キーブロック（ＥＫＢ）を使用してデバイスに配信する。

【０１００】例えば、図１２の例では、Ａ，またはＢのいずれかが他方が復号可能な有効化キーブロック（ＥＫＢ）を生成して生成した有効化キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して、他方に送信する構成としてもよいし、あるいは第３者がデバイスＡ，Ｂに対して双方が利用可能な有効化キーブロック（ＥＫＢ）を生成してデバイスＡ，Ｂに対して生成した有効化キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して配信する構成としてもよい。

【０１０１】図１３および図１４に複数のデバイスに共通の認証キーＫａｋｅを有効化キーブロック（ＥＫＢ）によって配信する構成例を示す。図１３はデバイス０，１，２，３に対して復号可能な認証キーＫａｋｅを配信する例、図１４はデバイス０，１，２，３中のデバイス３をリボーク（排除）してデバイス０，１，２に対してのみ復号可能な認証キーを配信する例を示す。

【０１０２】図１３の例では、更新ノードキーＫ（ｔ）００によって、認証キーＫａｋｅを暗号化したデータ（ｂ）とともに、デバイス０，１，２，３においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーＫ（ｔ）００を復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。それぞれのデバイスは、図１３の右側に示すようにまず、ＥＫＢを処理（復号）することにより、更新されたノードキーＫ（ｔ）００を取得し、次に、取得したノードキーＫ（ｔ）００を用いて暗号化された認証キー：Ｅｎｃ（Ｋ（ｔ）００，Ｋａｋｅ）を復号して認証キーＫａｋｅを得ることが可能となる。

【０１０３】その他のデバイス４，５，６，７…は同一の有効化キーブロック（ＥＫＢ）を受信しても自身の保有するノードキー、リーフキーでは、ＥＫＢを処理して更新されたノードキーＫ（ｔ）００を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【０１０４】一方、図１４の例は、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２，に対してのみ復号可能な有効化キーブロック（ＥＫＢ）を生成して配信した例である。図１４に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）認証キー（Ｋａｋｅ）をノードキー（Ｋ（ｔ）００）で暗号化したデータを配信する。

【０１０５】図１４の右側には、復号手順を示してある。デバイス０，１，２は、まず、受領した有効化キーブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号により認証キーＫａｋｅを取得する。

【０１０６】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【０１０７】このように、ＥＫＢを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

【０１０８】［公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信］次に、公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１５を用いて説明する。図１５において、公開鍵暗号方式としてＥＣＣを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１５において、まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび素数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。

【０１０９】Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。

【０１１０】次に、Ｂは、素数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（X座標とY座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１１１】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出

す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１１２】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッションキーとして以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

【０１１３】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１１４】図１６に公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとＰＣ間において図１５で説明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なＥＫＢを生成して、更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）とをＰＣ間の認証処理において生成したセッションキーＫｓｅｓで暗号化してＰＣに送信する。

【０１１５】ＰＣはセッションキーで暗号化された［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］をセッションキーで復号した後、再生装置、記録媒体に送信する。

【０１１６】再生装置、記録媒体は、自身の保有するノードキーまたはリーフキーによって［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］を復号することによってコンテンツキーＫｃｏｎを取得する。

【０１１７】この構成によれば、コンテンツプロバイダとＰＣ間での認証を条件として［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

【０１１８】［プログラムコードの有効化キーブロック（ＥＫＢ）を使用した配信］上述した例では、コンテンツキー、認証キー等を有効化キーブロック（ＥＫＢ）を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キーブロック（ＥＫＢ）を用いて配信する構成も可能である。すなわちＥＫＢによる暗号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

【０１１９】図１７にプログラムコードを有効化キーブロック（ＥＫＢ）の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス１７０１は、デバイス１７０２の有するノードキー、リーフキーによって復号可能な有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス１７０２に送信する。デバイス１７０２は受信したＥＫＢを処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコードを得る。

【０１２０】図１７に示す例では、さらに、デバイス１７０２において取得したプログラムコードによる処理を実行して、その結果をデバイス１７０１に返して、デバイス１７０１がその結果に基づいて、さらに処理を続行する例を示している。

【０１２１】このように有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図３で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

【０１２２】［送信コンテンツに対するチェック値（ＩＣＶ:Integrity Check Value）を対応させる構成］次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値（ＩＣＶ）を生成して、コンテンツに対応付けて、ＩＣＶの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

【０１２３】コンテンツのインテグリティ・チェック値（ＩＣＶ）は、例えばコンテンツに対するハッシュ関数を用いて計算され、ＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２，…）によって計算される。ＫｉｃｖはＩＣＶ生成キーである。Ｃ１，Ｃ２はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号（ＭＡＣ：Message authentication Code）が使用される。

【０１２４】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図１８に示す。図１８の構成に示すように対象となるメッセージを８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Cod

e））となる。

【０１２５】このようなコンテンツのＭＡＣ値とＩＣＶ生成キーにハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値（ＩＣＶ）が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成したＩＣＶと、新たにコンテンツに基づいて生成したＩＣＶとを比較して同一のＩＣＶが得られればコンテンツに改竄のないことが保証され、ＩＣＶが異なれば、改竄があったと判定される。

【０１２６】［チェック値（ＩＣＶ）の生成キーＫｉｃｖをＥＫＢによって配布する構成］次に、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであるＫｉｃｖを上述の有効化キーブロックによって送付する構成について説明する。すなわちＥＫＢによる暗号化メッセージデータをコンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーとした例である。

【０１２７】図１９および図２０に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キーＫｉｃｖを有効化キーブロック（ＥＫＢ）によって配信する構成例を示す。図１９はデバイス０，１，２，３に対して復号可能なチェック値生成キーＫｉｃｖを配信する例、図２０はデバイス０，１，２，３中のデバイス３をリボーク（排除）してデバイス０，１，２に対してのみ復号可能なチェック値生成キーＫｉｃｖを配信する例を示す。

【０１２８】図１９の例では、更新ノードキーＫ（ｔ）００によって、チェック値生成キーＫｉｃｖを暗号化したデータ（ｂ）とともに、デバイス０，１，２，３においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーＫ（ｔ）００を復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。それぞれのデバイスは、図１９の右側に示すようにまず、ＥＫＢを処理（復号）することにより、更新されたノードキーＫ（ｔ）００を取得し、次に、取得したノードキーＫ（ｔ）００を用いて暗号化されたチェック値生成キー：Ｅｎｃ（Ｋ（ｔ）００，Ｋｉｃｖ）を復号してチェック値生成キーＫｉｃｖを得ることが可能となる。

【０１２９】その他のデバイス４，５，６，７…は同一の有効化キーブロック（ＥＫＢ）を受信しても自身の保有するノードキー、リーフキーでは、ＥＫＢを処理して更新されたノードキーＫ（ｔ）００を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【０１３０】一方、図２０の例は、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２，に対してのみ復号可能な有効化キーブロック（ＥＫＢ）を生成して配信した例である。図２０に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）チェック値生成キー（Ｋｉｃｖ）をノードキー（Ｋ（ｔ）００）で暗号化したデータを配信する。

【０１３１】図２０の右側には、復号手順を示してある。デバイス０，１，２は、まず、受領した有効化キーブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号によりチェック値生成キーＫｉｃｖを取得する。

【０１３２】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【０１３３】このように、ＥＫＢを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【０１３４】このようなコンテンツのインテグリティ・チェック値（ＩＣＶ）を用いることにより、ＥＫＢと暗号化コンテンツの不正コピーを排除することができる。例えば図２１に示すように、コンテンツＣ１とコンテンツＣ２とをそれぞれのコンテンツキーを取得可能な有効化キーブロック（ＥＫＢ）とともに格納したメディア１があり、これをそのままメディア２にコピーした場合を想定する。ＥＫＢと暗号化コンテンツのコピーは可能であり、これをＥＫＢを復号可能なデバイスでは利用できることになる。

【０１３５】図２１の（ｂ）に示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値（ＩＣＶ（Ｃ１，Ｃ２））を格納する構成とする。なお、（ＩＣＶ（Ｃ１，Ｃ２））は、コンテンツＣ１とコンテンツＣ２にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値であるＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２）を示している。図２１の（ｂ）の構成において、メディア１には正当にコンテンツ１とコンテンツ２が格納され、コンテンツＣ１とコンテンツＣ２に基づいて生成されたインテグリティ・チェック値（ＩＣＶ（Ｃ１，Ｃ２））が格納される。また、メディア２には正当にコンテンツ１が格納され、コンテンツＣ１に基づいて生成されたインテグリティ・チェック値（ＩＣＶ（Ｃ１））が格納される。この構成において、メディア１に格納された｛ＥＫＢ，コンテンツ２｝をメディア２にコピーしたとすると、メディア２で、コンテンツチェック値を新たに生成するとＩＣＶ（Ｃ１，Ｃ２）が生成されることになり、メディア

に格納されているＫｉｃｖ（Ｃ１）と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにＩＣＶチェックを実行して、生成ＩＣＶと格納ＩＣＶの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

【０１３６】また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値（ＩＣＶ）を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわちＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，ｃｏｕｎｔｅｒ＋１，Ｃ１，Ｃ２，…）によって計算する構成とする。ここで、カウンタ（ｃｏｕｎｔｅｒ＋１）は、ＩＣＶの書き換えごとに１つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【０１３７】さらに、コンテンツのインテグリティ・チェック値（ＩＣＶ）をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値（ＩＣＶ）をコンテンツとは別のメディア上に格納する構成としてもよい。

【０１３８】例えば、読み込み専用メディアや通常のＭＯ等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値（ＩＣＶ）を格納するとＩＣＶの書き換えが不正なユーザによりなされる可能性があり、ＩＣＶの安全性が保てないおそれがある。この様な場合、ホストマシン上の安全なメディアにＩＣＶを格納して、コンテンツのコピーコントロール（例えばcheck-in/check-out、move）にＩＣＶを使用する構成とすることにより、ＩＣＶの安全な管理およびコンテンツの改竄チェックが可能となる。

【０１３９】この構成例を図２２に示す。図２２では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア２２０１にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値（ＩＣＶ）を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア２２０２に格納し、ユーザによる不正なインテグリティ・チェック値（ＩＣＶ）の書き換えを防止した例である。このような構成として、例えばメディア２２０１を装着したデバイスがメディア２２０１の再生を実行する際にホストマシンであるＰＣ、サーバにおいてＩＣＶのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

【０１４０】［階層ツリー構造のカテゴリー分類］暗号鍵をルートキー、ノードキー、リーフキー等、図３の階層ツリー構造として構成し、コンテンツキー、認証キー、ＩＣＶ生成キー、あるいはプログラムコード、データ等を有効化キーブロック（ＥＫＢ）とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリー毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【０１４１】図２３に階層ツリー構造のカテゴリーの分類の一例を示す。図２３において、階層ツリー構造の最上段には、ルートキーＫｒｏｏｔ２３０１が設定され、以下の中間段にはノードキー２３０２が設定され、最下段には、リーフキー２３０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【０１４２】ここで、一例として最上段から第M段目のあるノードをカテゴリノード２３０４として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の１つのノードを頂点として以下、Ｍ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【０１４３】例えば図２３の第M段目の１つのノード２３０５にはカテゴリ［メモリステッイク（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード２３０５以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【０１４４】さらに、M段から数段分下位の段をサブカテゴリノード２３０６として設定することができる。例えば図に示すようにカテゴリ［メモリスティック］ノード２３０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード２３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード２３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード２３０８と［携帯電話］ノード２３０９を設定することができる。

【０１４５】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下

段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【０１４６】このように、１つのノードを頂点としして、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【０１４７】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１４８】

【発明の効果】以上、説明したように、本発明の情報処理システムおよび方法によれば、ツリー（木）構造の鍵配布構成により、コンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等を有効化キーブロック（ＥＫＢ）とともに送信する構成としたので、正当なデバイスにおいてのみ復号可能な暗号データ配信が可能となるとともに配信メッセージ量を小さく押さえることができる。

【０１４９】また、ツリー構造の暗号化キー、データ配信方式を用いてコンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等を有効化キーブロック（ＥＫＢ）とともに送信する構成において、さらに、共通鍵方式、あるいは公開鍵方式の認証処理を併用する構成とすれば、さらに安全なデータ配信が可能となる。

【０１５０】また、本発明の情報処理システムおよび方法によれば、コンテンツに対するインテグリティ・チェック値（ＩＣＶ）をコンテンツを格納した記録媒体、あるいはその他のメディアに格納してコンテンツ改竄のチェック、あるいはコピーチェックを可能としたので、不正なコンテンツの流通を防止することが可能となる。

【０１５１】また、本発明の情報処理システムおよび方法によれば、ツリー構造の暗号化キー、データ配信方式において、階層ツリーをカテゴリ毎に分類して、各カテゴリの管理する頂点ノード以下のノード、リーフを特定のデバイスに限定する構成としたので、各カテゴリの管理者が独自に有効化キーブロック（ＥＫＢ）を生成して管理下にあるデバイスに対して配信することが可能となる。

【図面の簡単な説明】

【図１】本発明の情報処理システムの構成例を説明する図である。

【図２】本発明の情報処理システムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

【図３】本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図４】本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図５】本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

【図６】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

【図７】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

【図８】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図９】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

【図１０】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）とコンテンツを記録媒体に格納した場合の対応について説明する図である。

【図１１】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキーを送付する処理を従来の送付処理と比較した図である。

【図１２】本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

【図１３】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その１）である。

【図１４】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その２）である。

【図１５】本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

【図１６】本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キーブロック（ＥＫＢ）と、コンテンツキーを併せて配信する処理を示す図である。

【図１７】本発明の情報処理システムにおいて有効化キーブロック（ＥＫＢ）と、暗号化プログラムデータを併せて配信する処理を示す図である。

【図１８】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）の生成に使用するＭＡＣ値生成例を示す図である。

【図１９】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、ＩＣＶ生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その１）である。

【図２０】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、ＩＣＶ生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その２）である。

【図２１】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）をメディアに格納した場合のコピー防止機能を説明する図である。

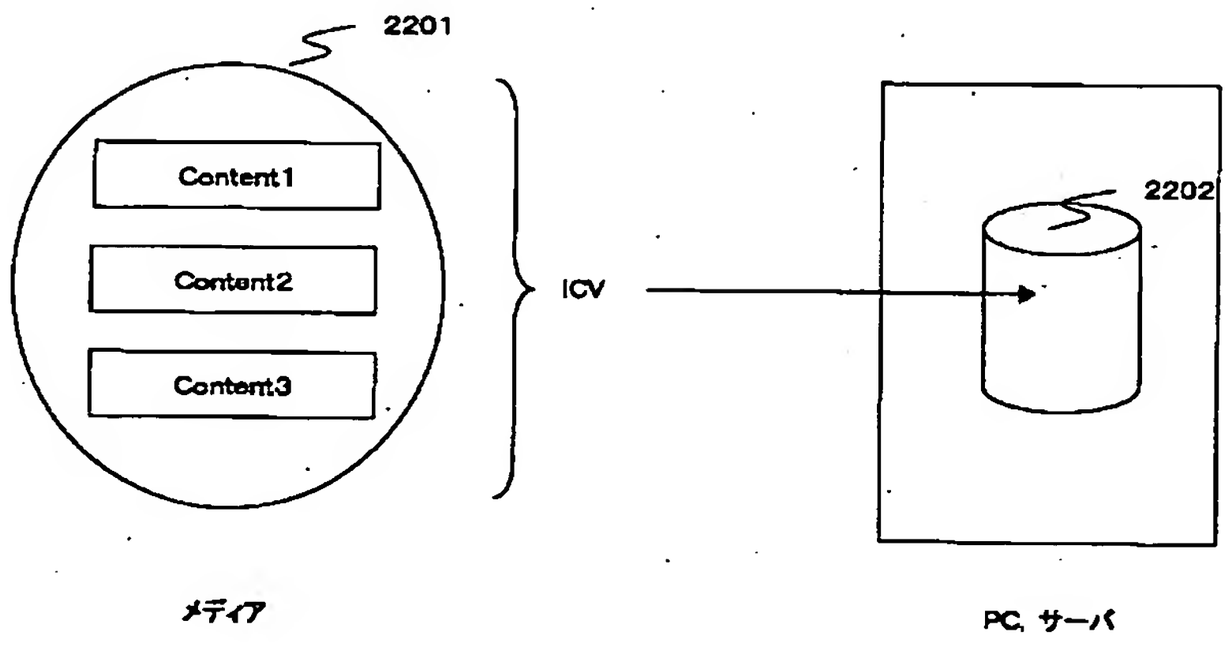
【図２２】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）をコンテンツ格納媒体と別に管理する構成を説明する図である。

【図２３】本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

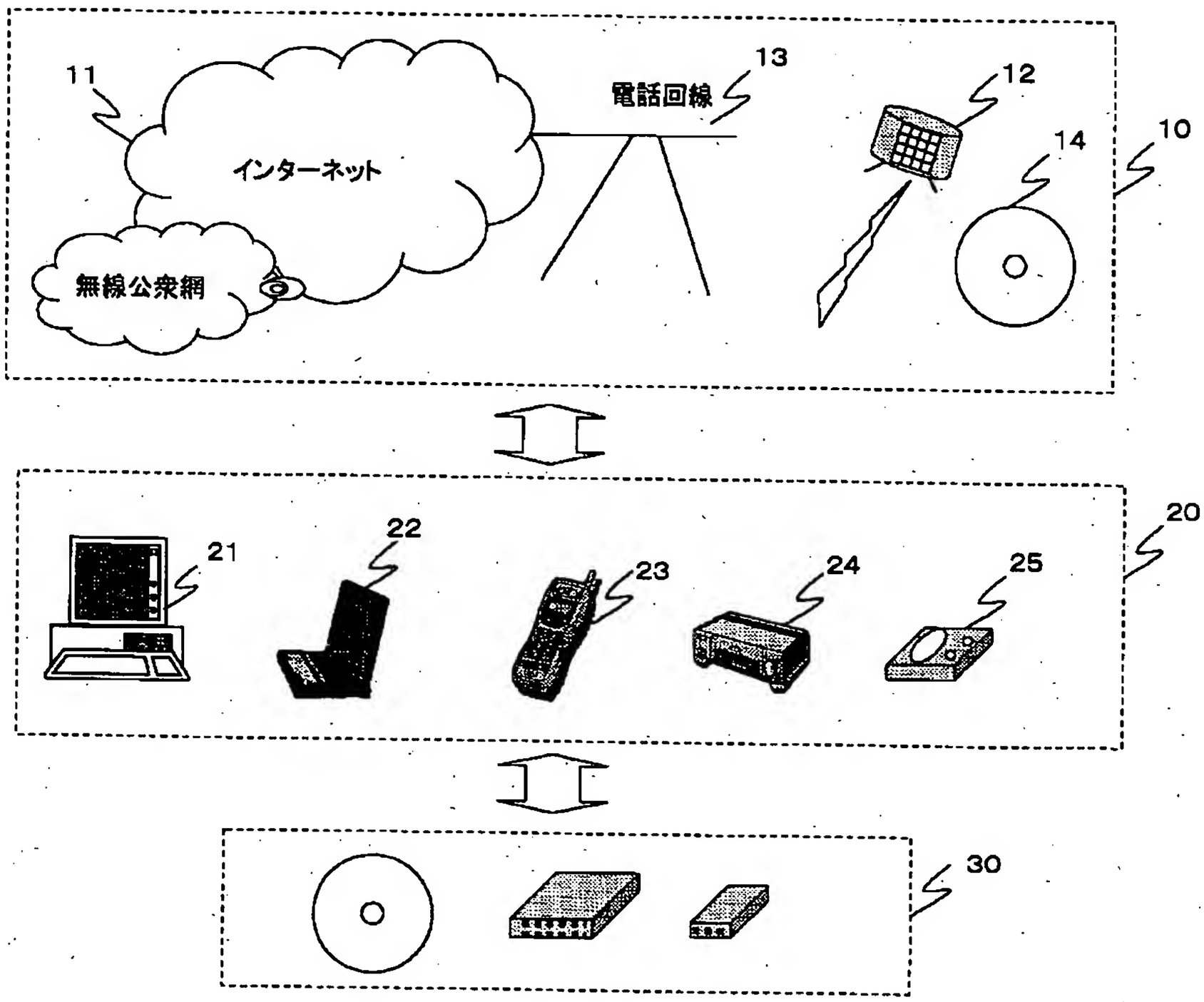
【符号の説明】

１０　コンテンツ配信側
１１　インターネット
１２　衛星放送
１３　電話回線
１４　メディア
２０　コンテンツ受信側
２１　パーソナルコンピュータ（ＰＣ）
２２　ポータブルデバイス（ＰＤ）
２３　携帯電話、ＰＤＡ
２４　記録再生器
２５　再生専用器
３０　メディア
１００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　ドライブ
１９５　記録媒体
６０１　バージョン
６０２　デプス
６０３　データポインタ
６０４　タグポインタ
６０５　署名ポインタ
６０６　データ部
６０７　タグ部
６０８　署名
１１０１　記録デバイス
２３０１　ルートキー
２３０２　ノードキー
２３０３　リーフキー
２３０４　カテゴリノード
２３０６　サブカテゴリノード

【図２２】



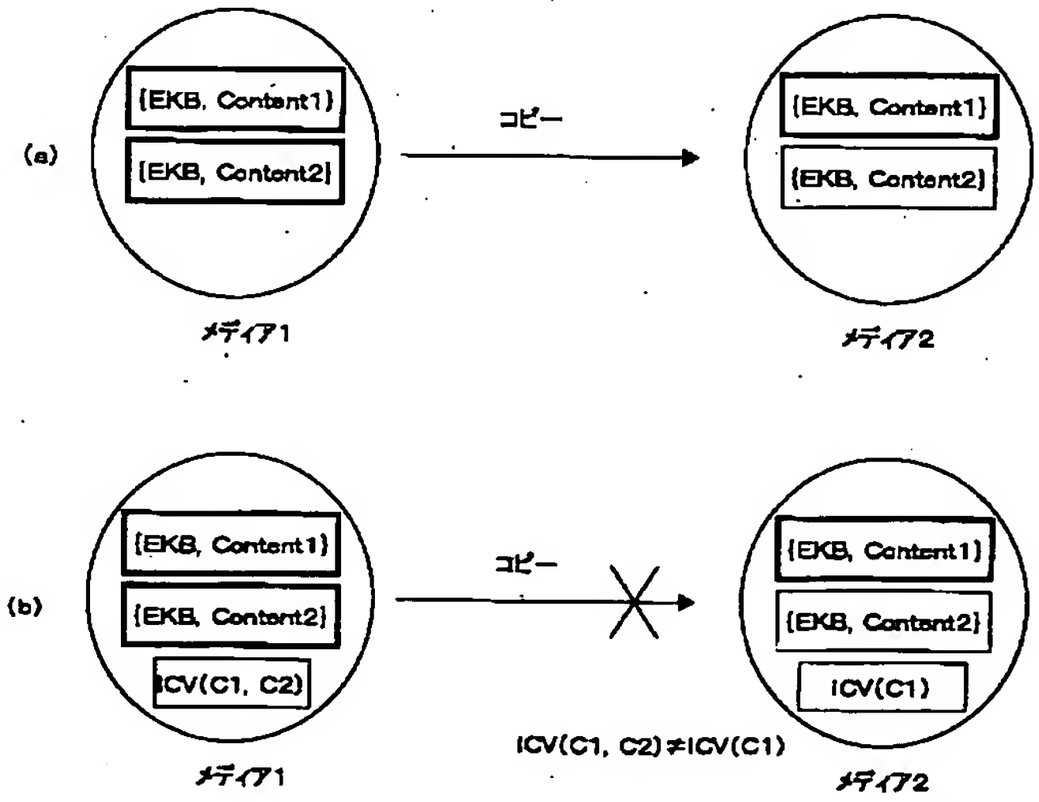
【図１】


11
インターネット
無線公衆網
13
電話回線
12
14
10
20
21
22
23
24
25
30

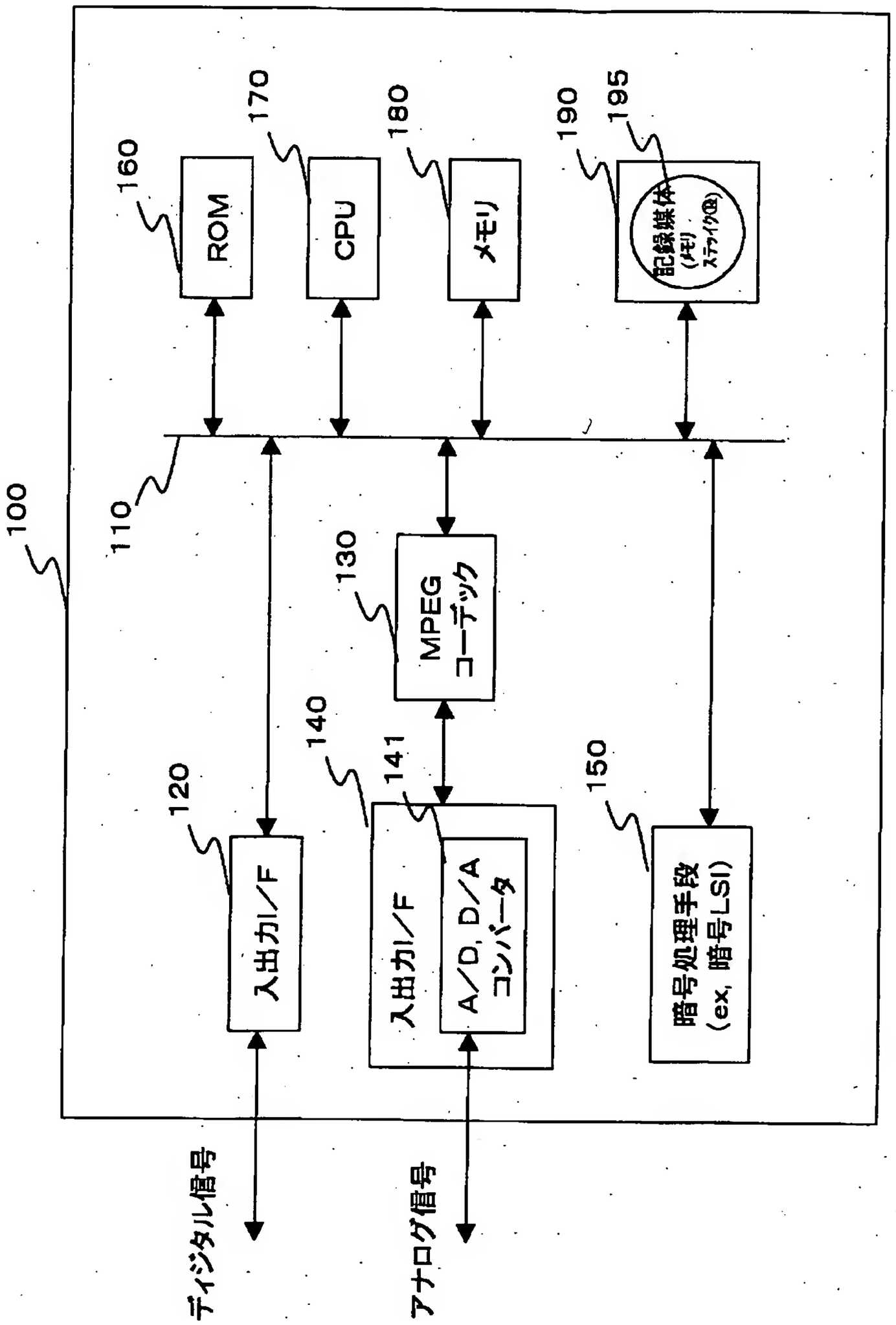
【図１０】


格納コンテンツ
コンテンツ:C1
コンテンツ:C2
コンテンツ:C3
コンテンツ:C4
格納EKB
EKB_M
対応付けデータ
<コンテンツ:C1 EKB_1>
<コンテンツ:C2 EKB_2>
<コンテンツ:C3 EKB_M>
<コンテンツ:C4 EKB_M>
記録媒体

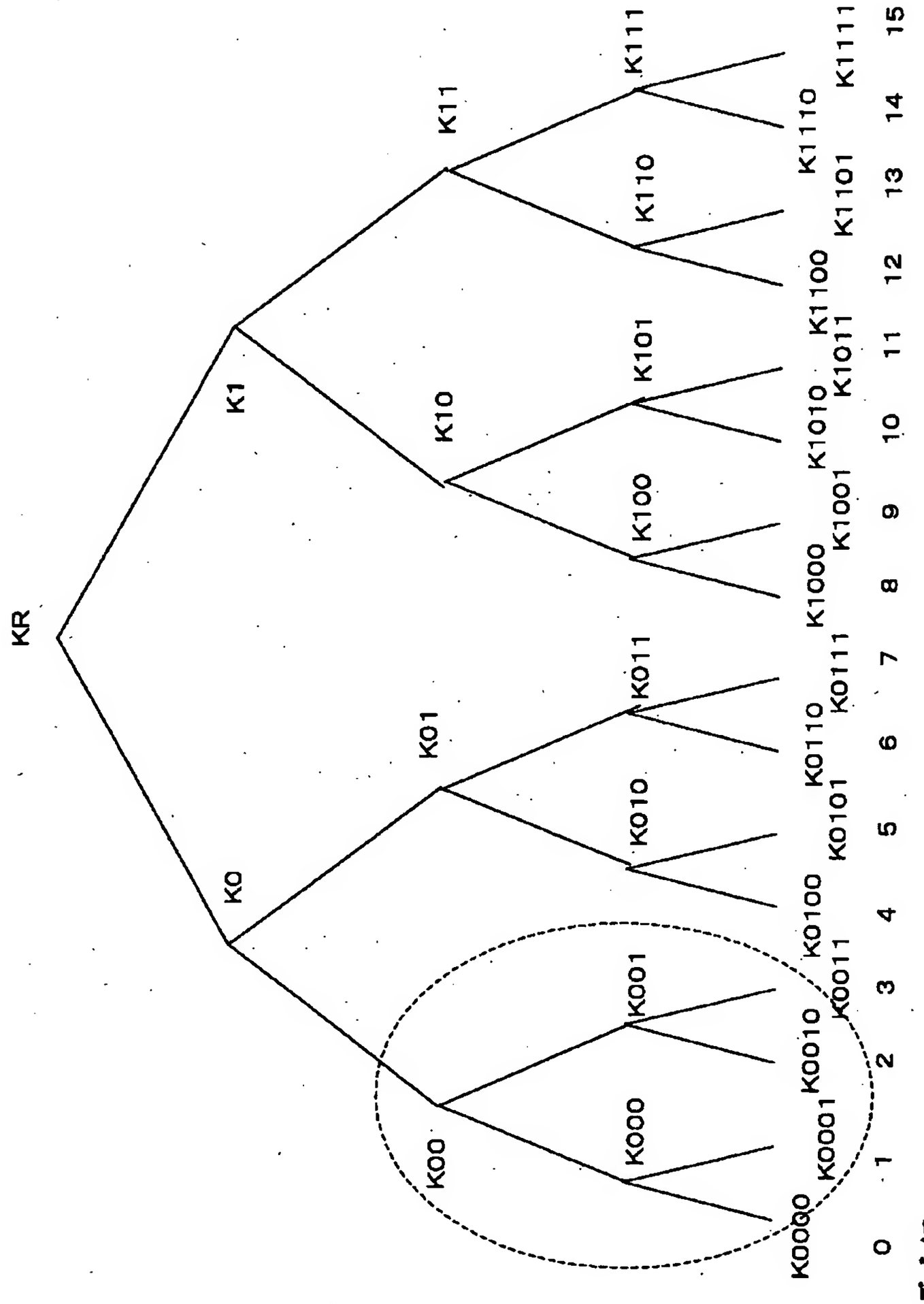
【図２１】


(a)
{EKB, Content1}
{EKB, Content2}
コピー
{EKB, Content1}
{EKB, Content2}
メディア1
メディア2
(b)
{EKB, Content1}
{EKB, Content2}
ICV(C1, C2)
コピー
{EKB, Content1}
{EKB, Content2}
ICV(C1)
ICV(C1, C2)≠ICV(C1)
メディア1
メディア2

【図２】


100
110
160
ROM
170
CPU
180
メモリ
190
195
記録媒体
(メモリ
スティック(登録商標))
130
MPEG
コーデック
120
入出力I／F
140
141
入出力I／F
A／D, D／A
コンバータ
150
暗号処理手段
(ex, 暗号LSI)
ディジタル信号
アナログ信号

【図３】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
レベル

【図４】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

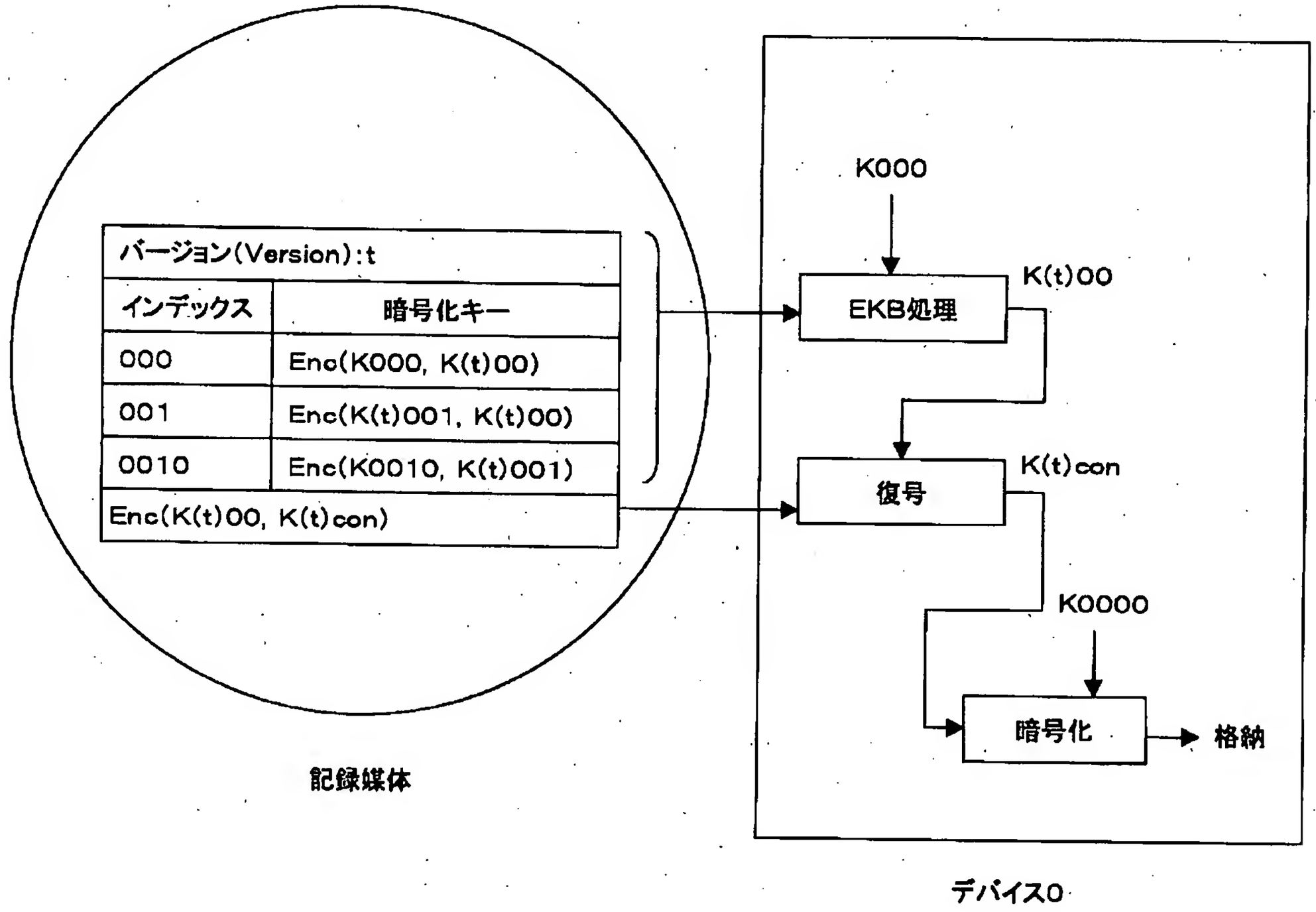
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

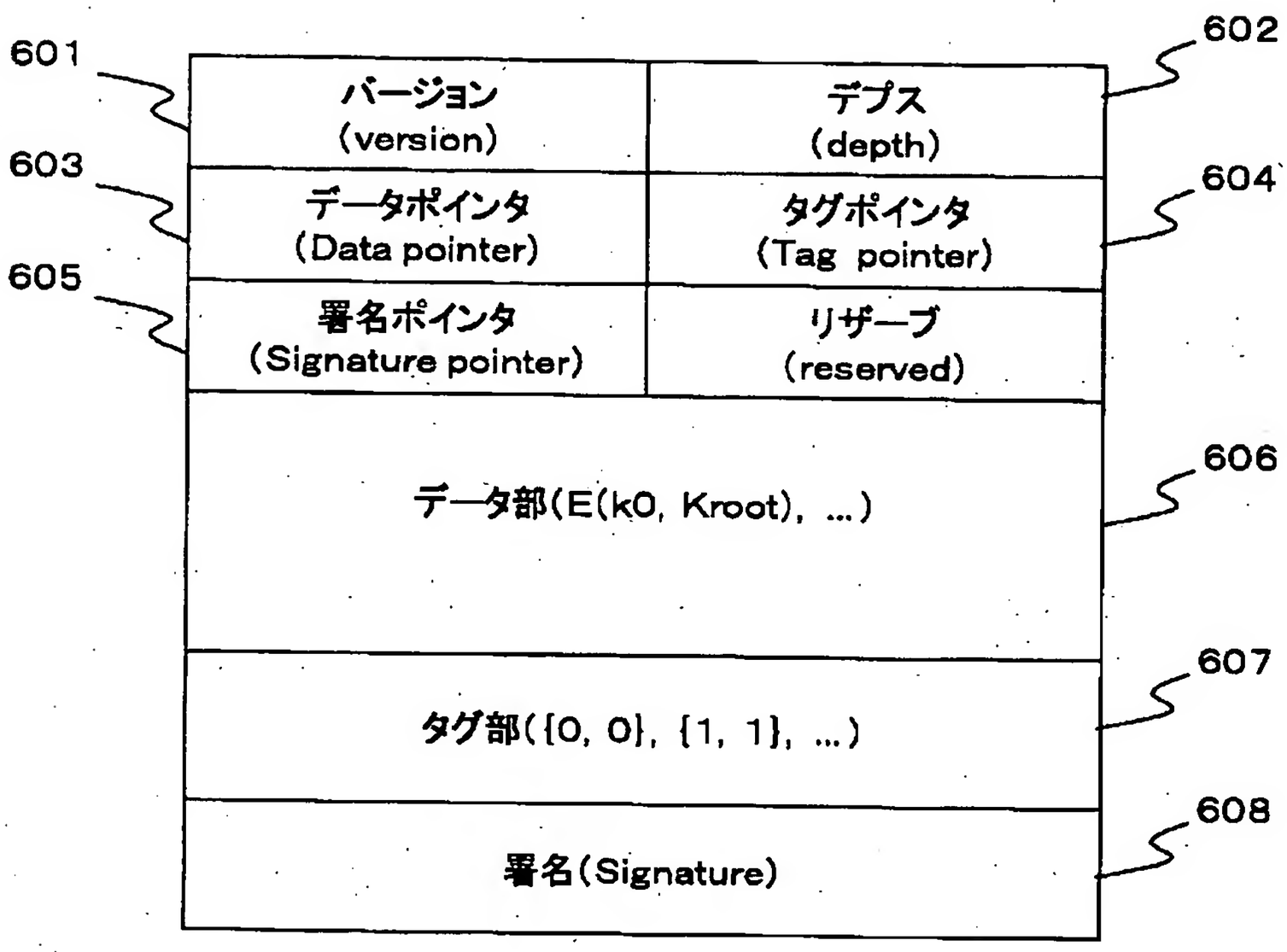
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

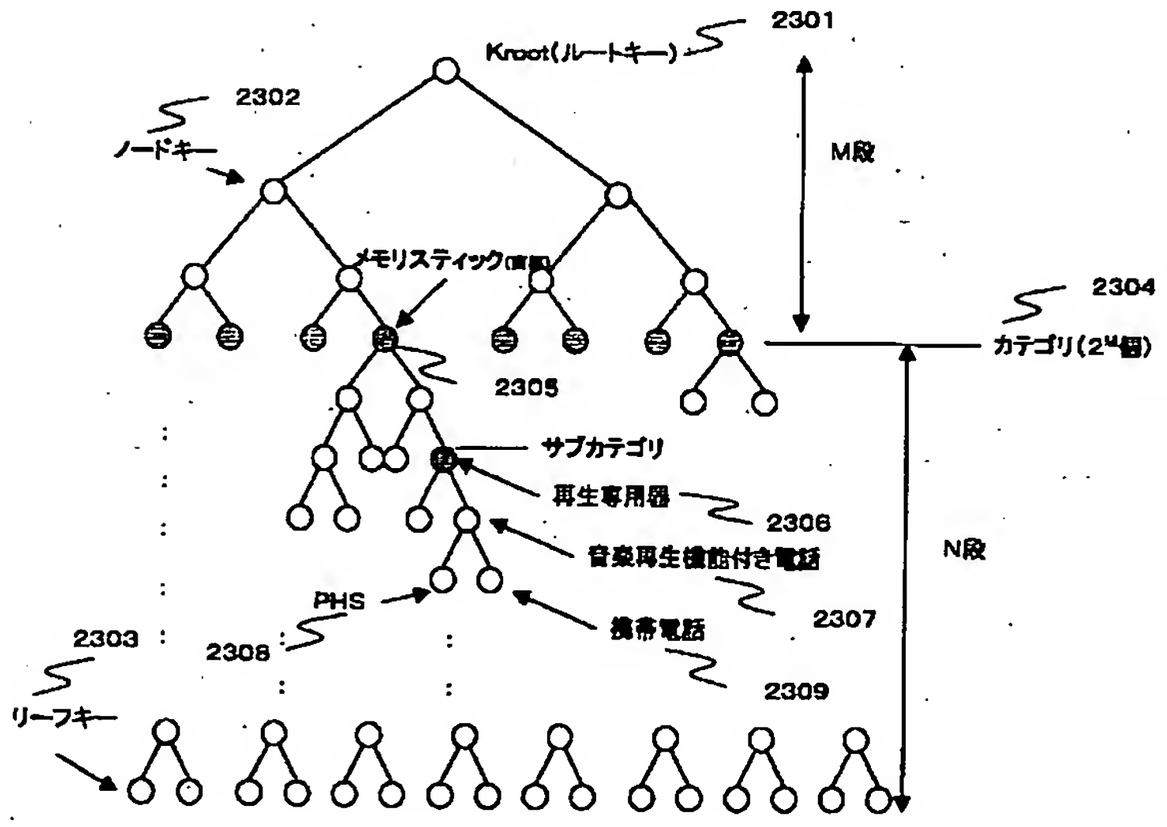

バージョン(Version):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
記録媒体
K000
EKB処理
K(t)00
復号
K(t)con
K0000
暗号化
格納
デバイスD

【図5】

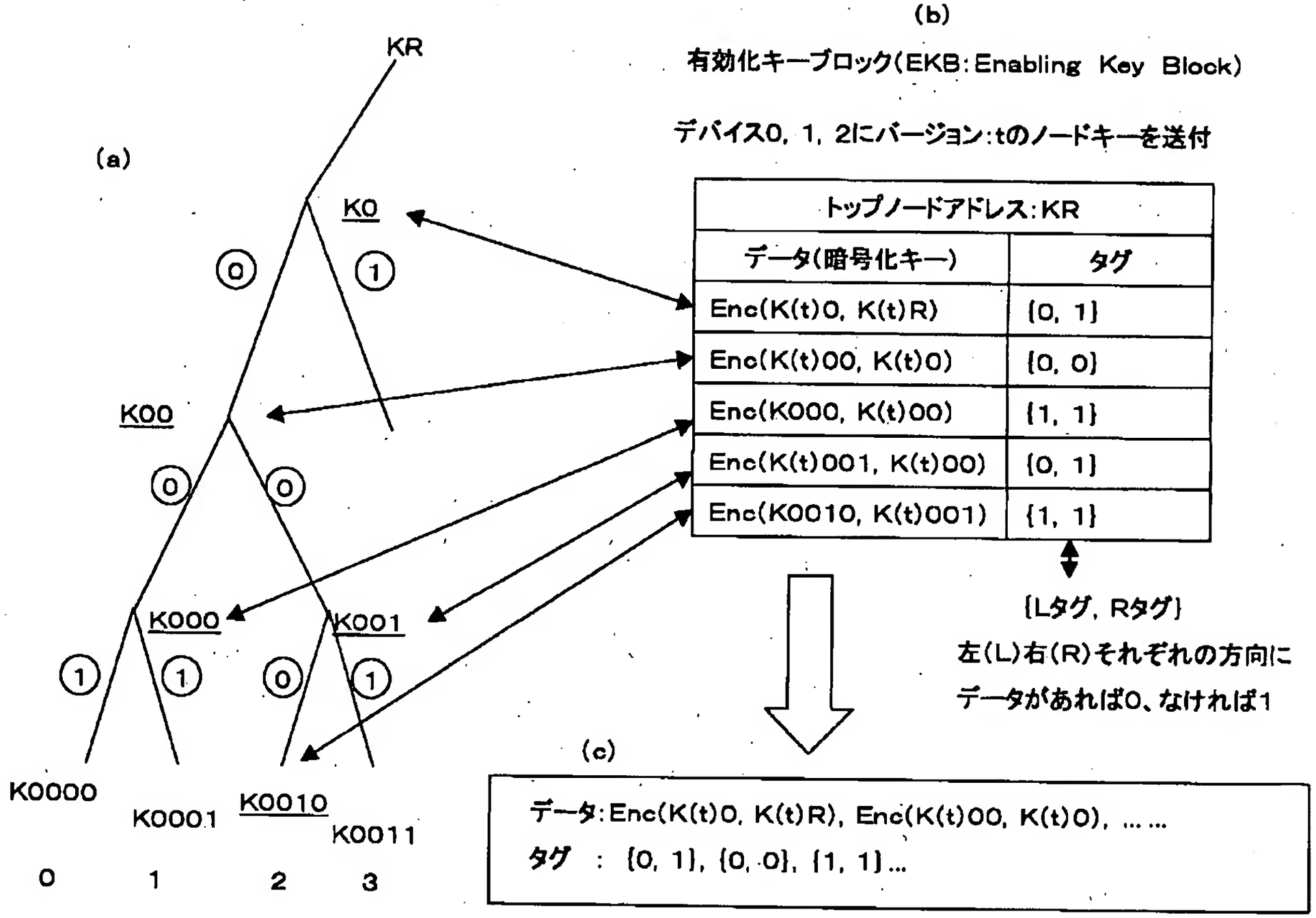
【図６】


601
602
バージョン
(version)
デプス
(depth)
603
604
データポインタ
(Data pointer)
タグポインタ
(Tag pointer)
605
署名ポインタ
(Signature pointer)
リザーブ
(reserved)
606
データ部(E(k0, Kroot), ...)
607
タグ部({0, 0}, {1, 1}, ...)
608
署名(Signature)

【図２３】

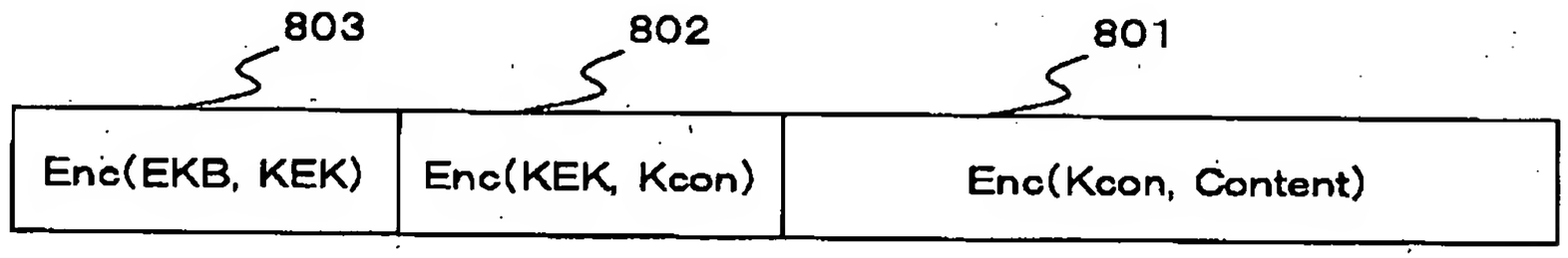

2301
Kroot(ルートキー)
2302
ノードキー
M段
メモリスティック(商標)
2304
カテゴリ(2^M個)
2305
サブカテゴリ
再生専用器
2306
音楽再生機能付き電話
N段
PHS
2307
携帯電話
2303
2308
2309
リーフキー

【図7】

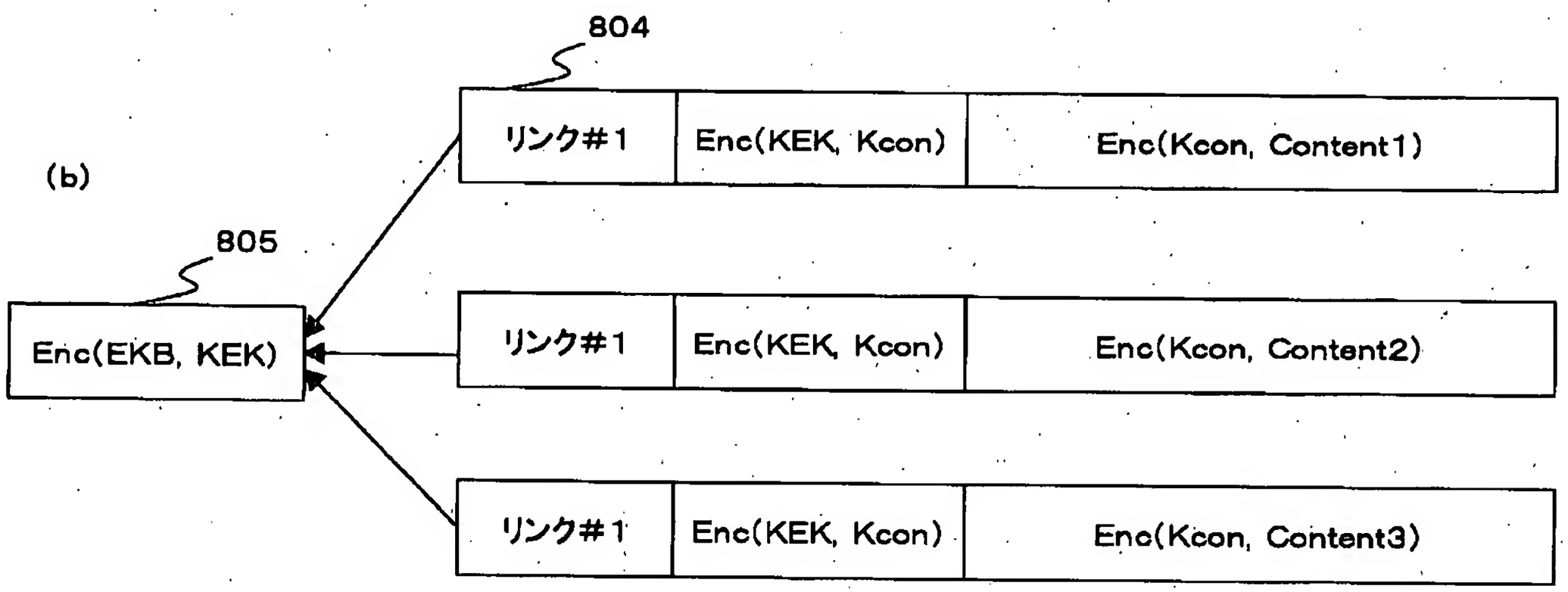

(a)
KR
K0
0
1
K00
0
0
K000
K001
1
1
0
1
K0000
K0001
K0010
K0011
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
タグ : {0, 1}, {0, 0}, {1, 1}…

【図8】

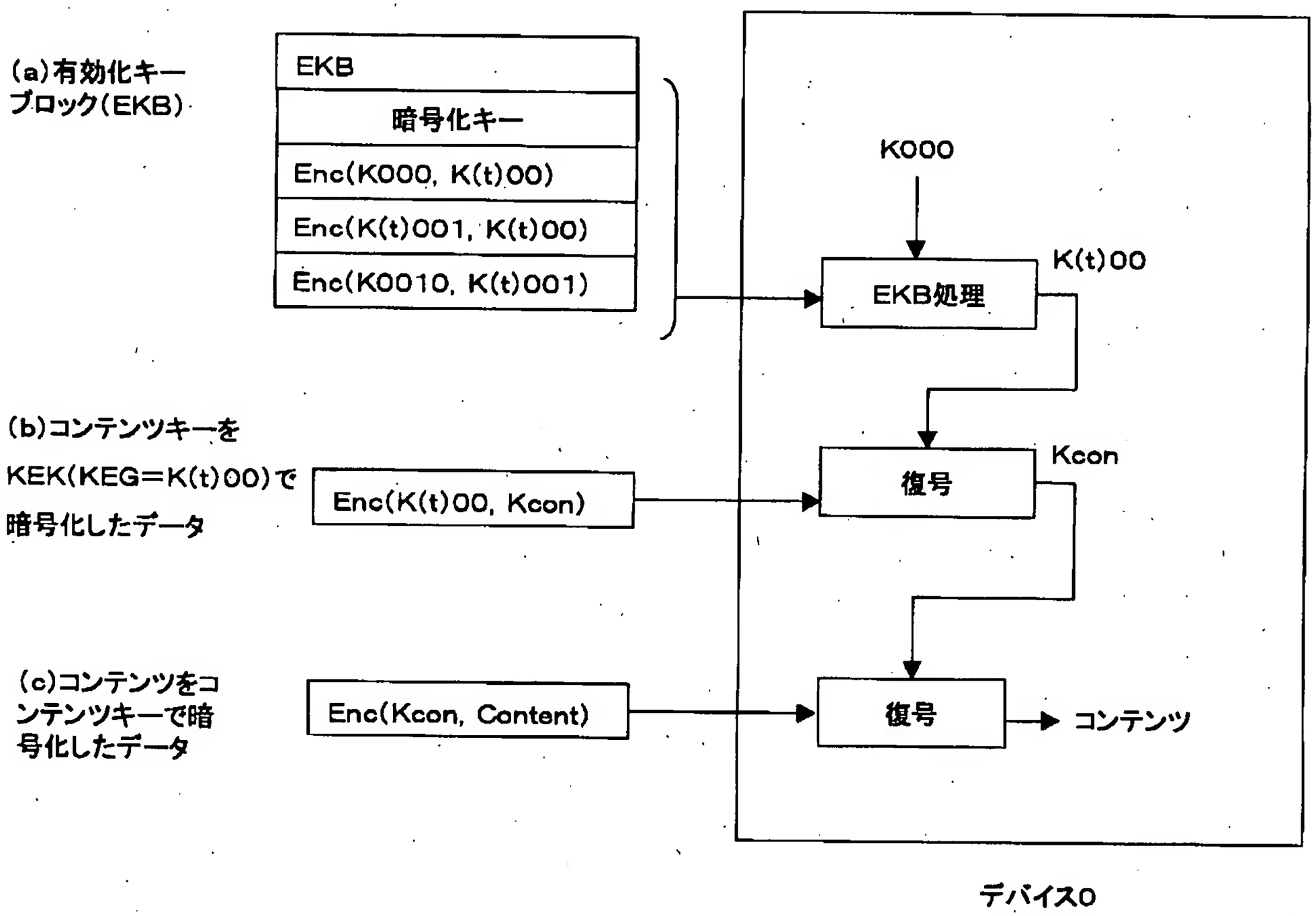
(a)


803
802
801
Enc(EKB, KEK)
Enc(KEK, Kcon)
Enc(Kcon, Content)

(b)

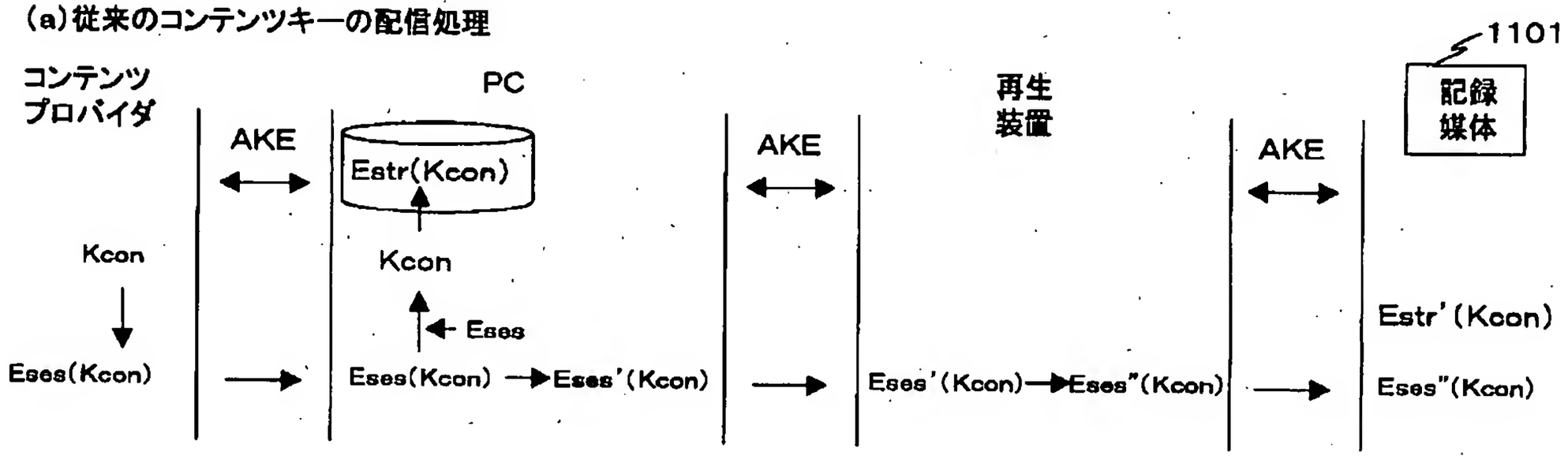

804
805
Enc(EKB, KEK)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content2)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content3)

【図9】

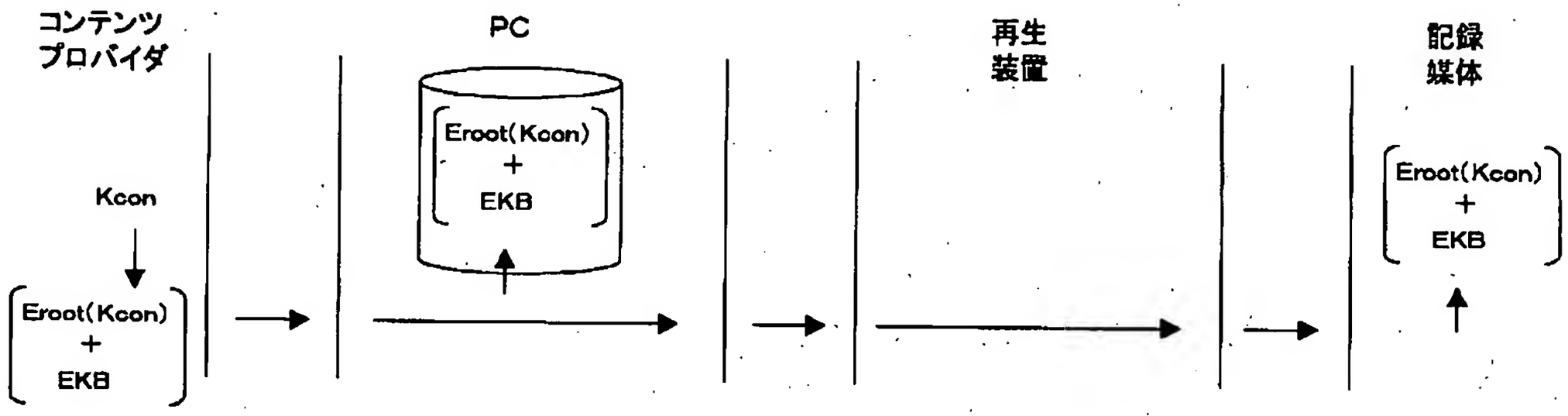

(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K000
EKB処理
K(t)00
復号
Kcon
(b)コンテンツキーをKEK(KEG=K(t)00)で暗号化したデータ
Enc(K(t)00, Kcon)
(c)コンテンツをコンテンツキーで暗号化したデータ
Enc(Kcon, Content)
復号
コンテンツ
デバイス0

【図11】

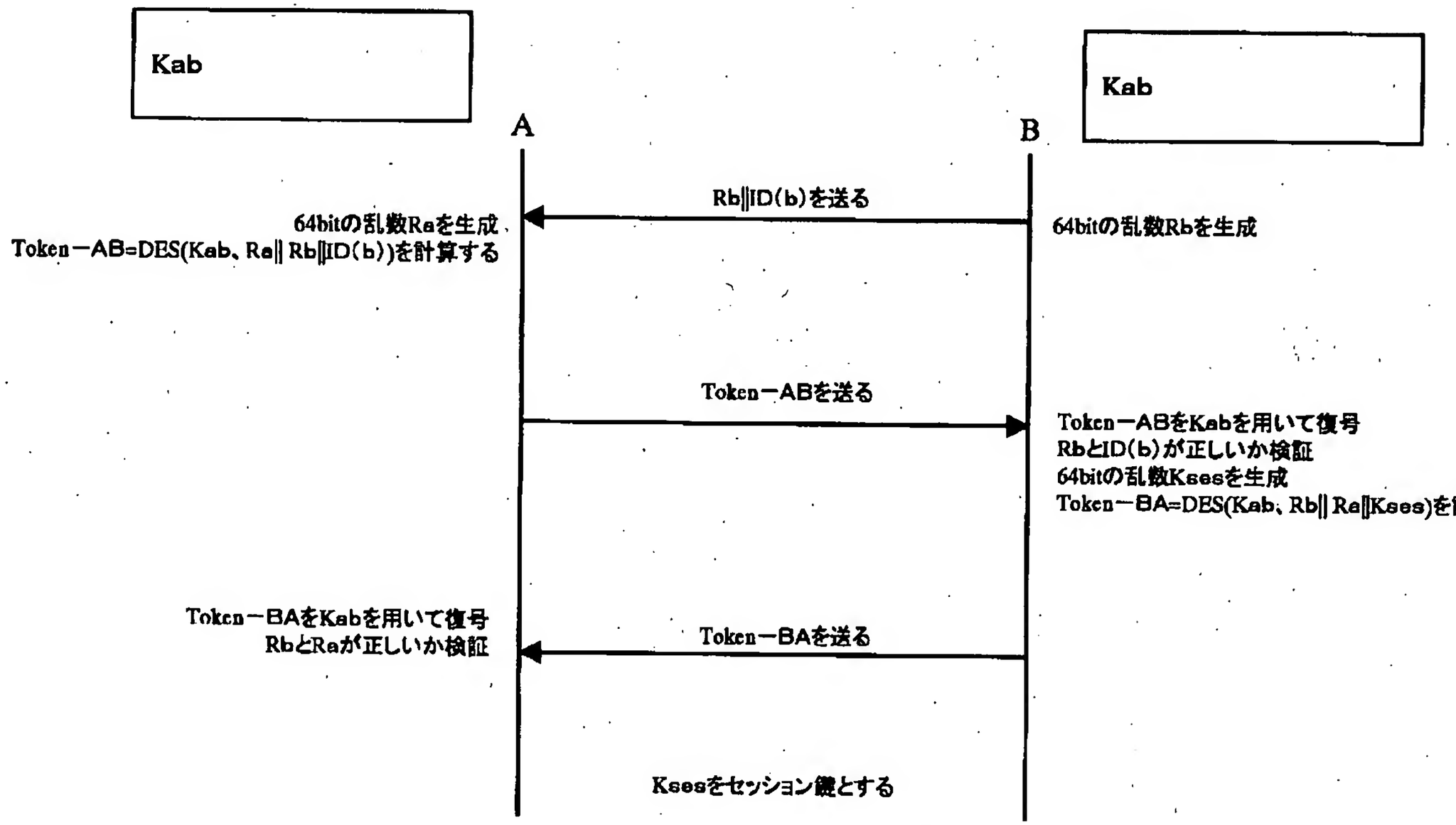
(a)従来のコンテンツキーの配信処理



(b)有効化キーブロック(EKB)を利用した
コンテンツキーの配信処理

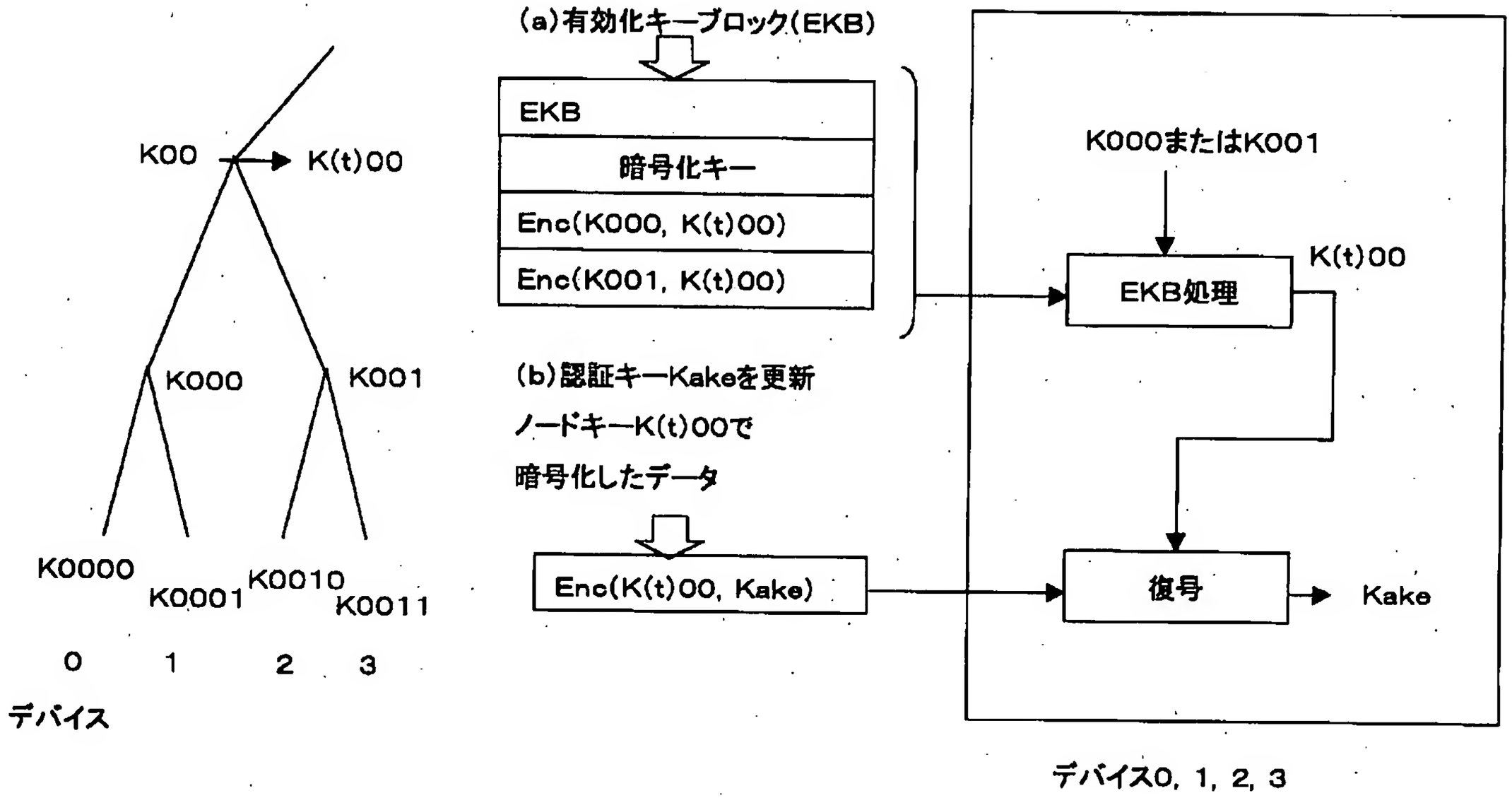


【図１２】

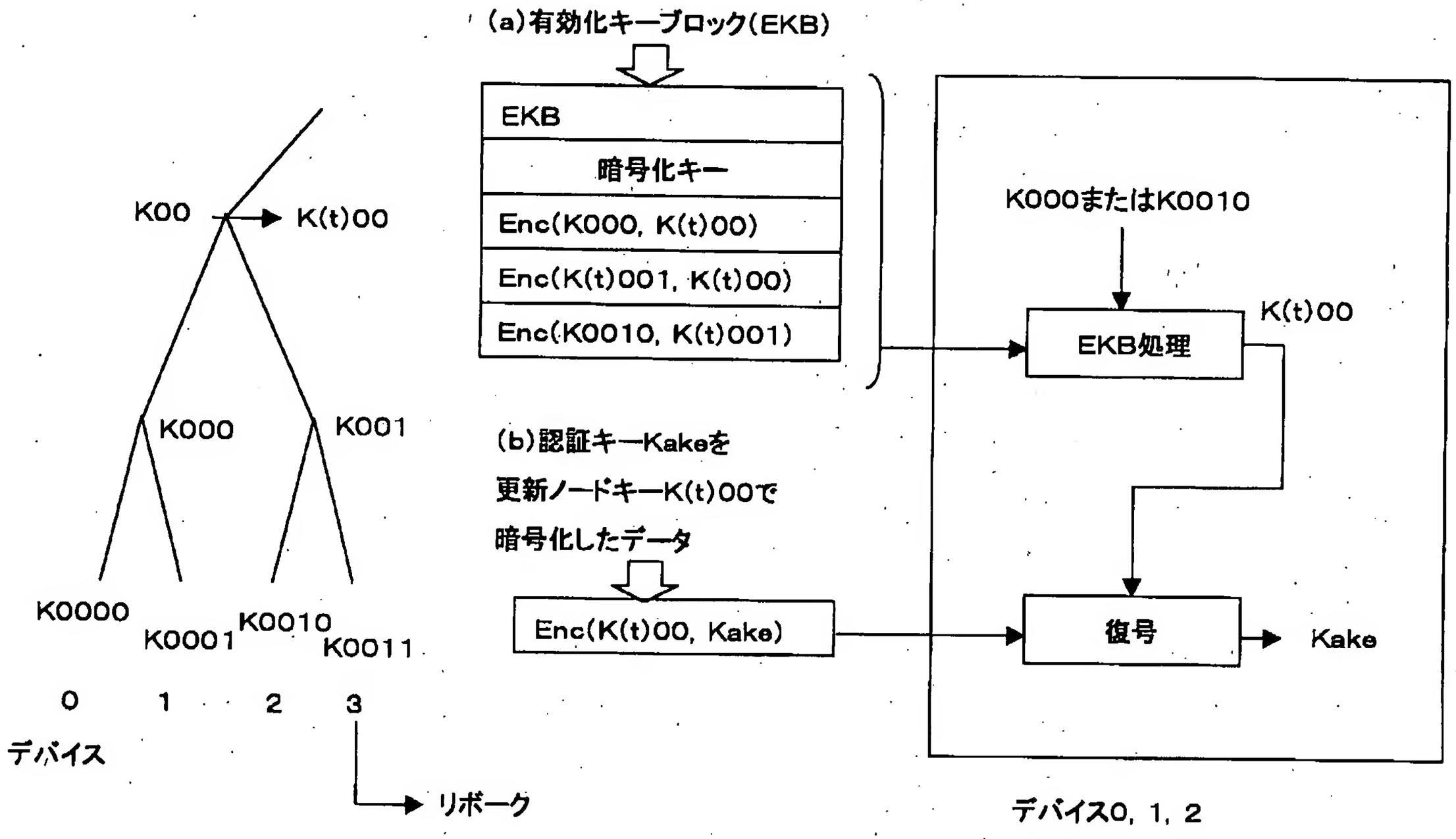


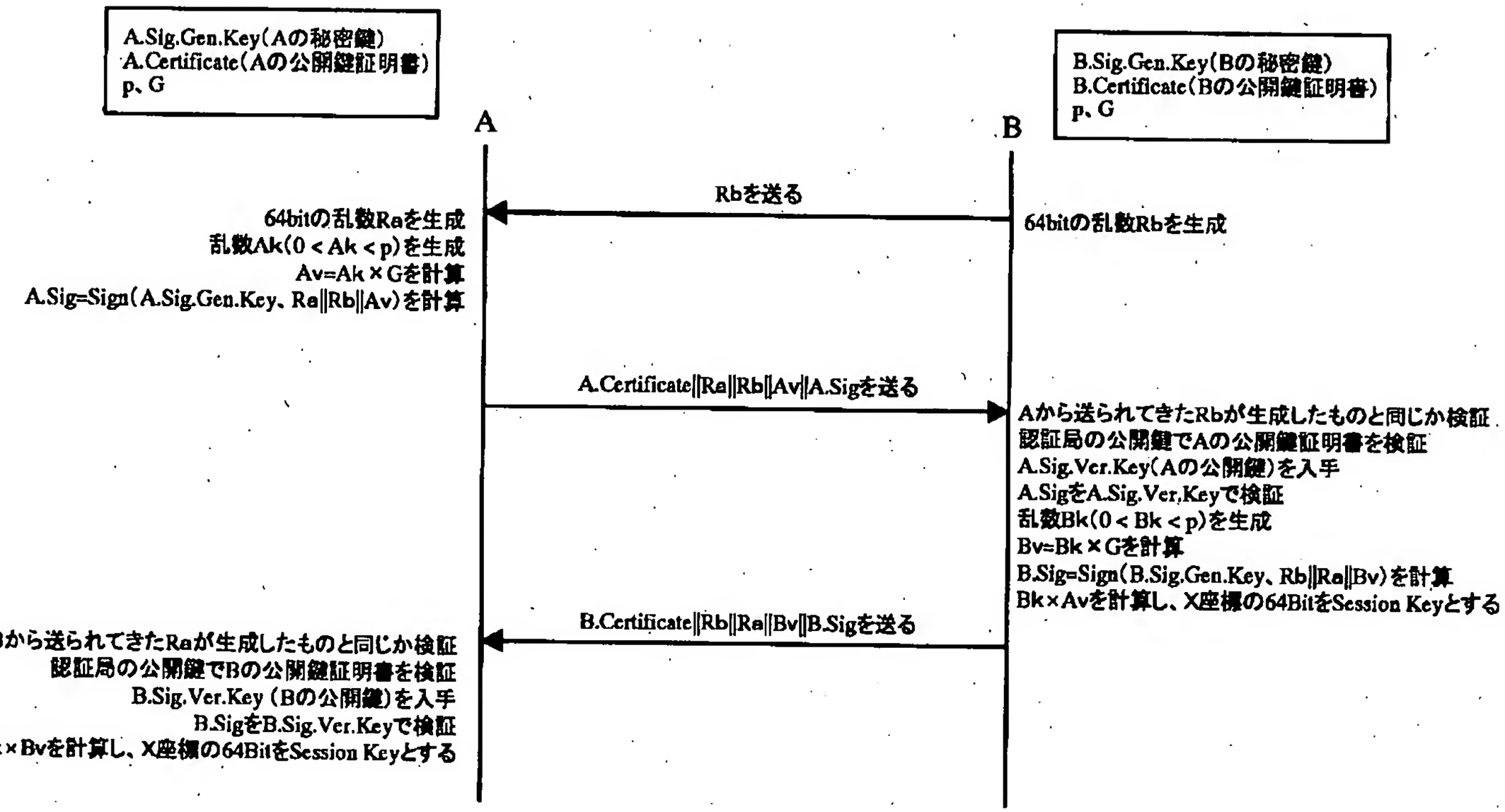
ISO/IEC 9798-2　対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１３】


K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
デバイス
(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K001, K(t)00)
(b)認証キーKakeを更新
ノードキーK(t)00で
暗号化したデータ
Enc(K(t)00, Kake)
K000またはK001
EKB処理
K(t)00
復号
Kake
デバイス0, 1, 2, 3

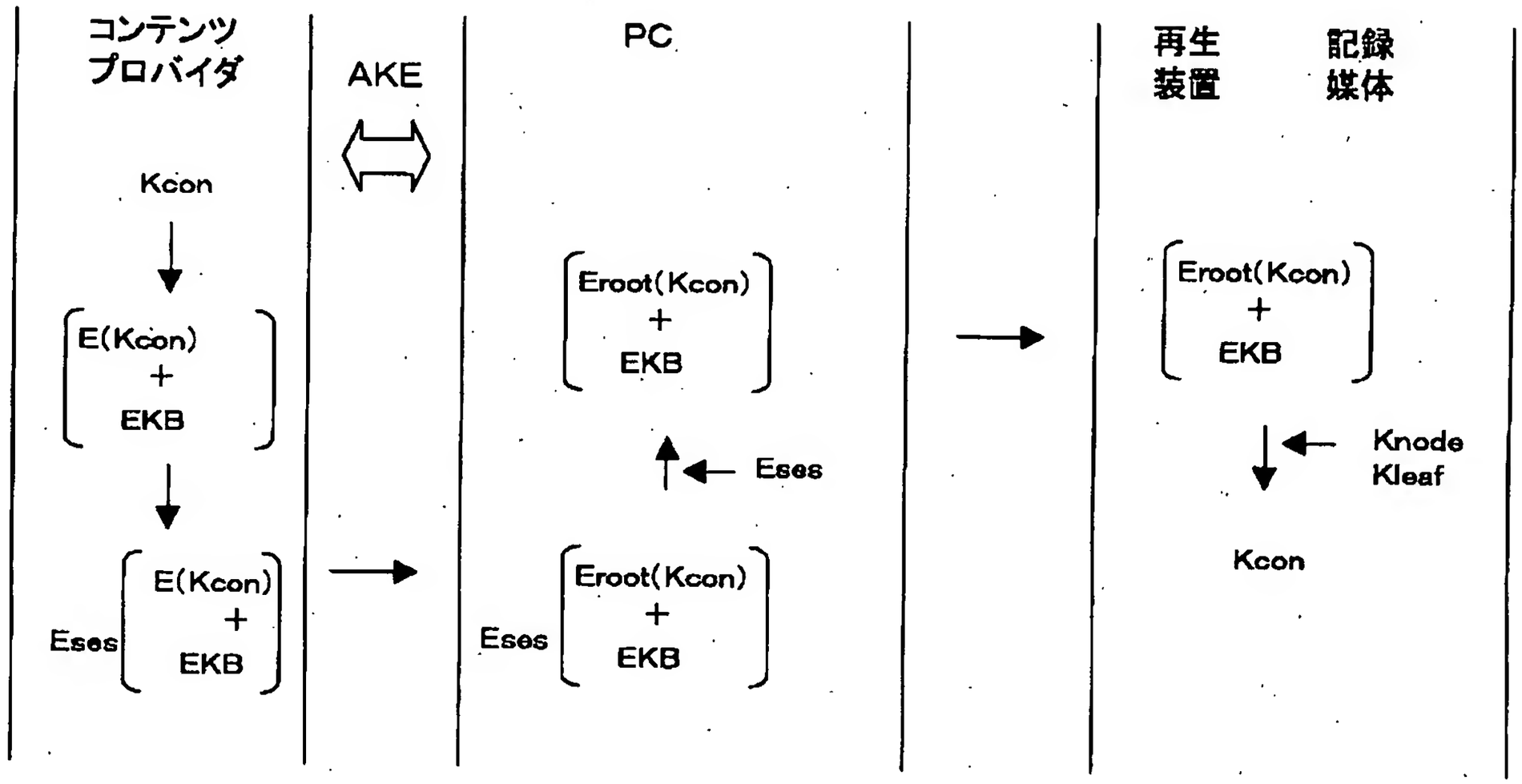
【図14】


(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
デバイス
リボーク
(b)認証キーKakeを
更新ノードキーK(t)00で
暗号化したデータ
Enc(K(t)00, Kake)
K000またはK0010
EKB処理
K(t)00
復号
Kake
デバイス0, 1, 2



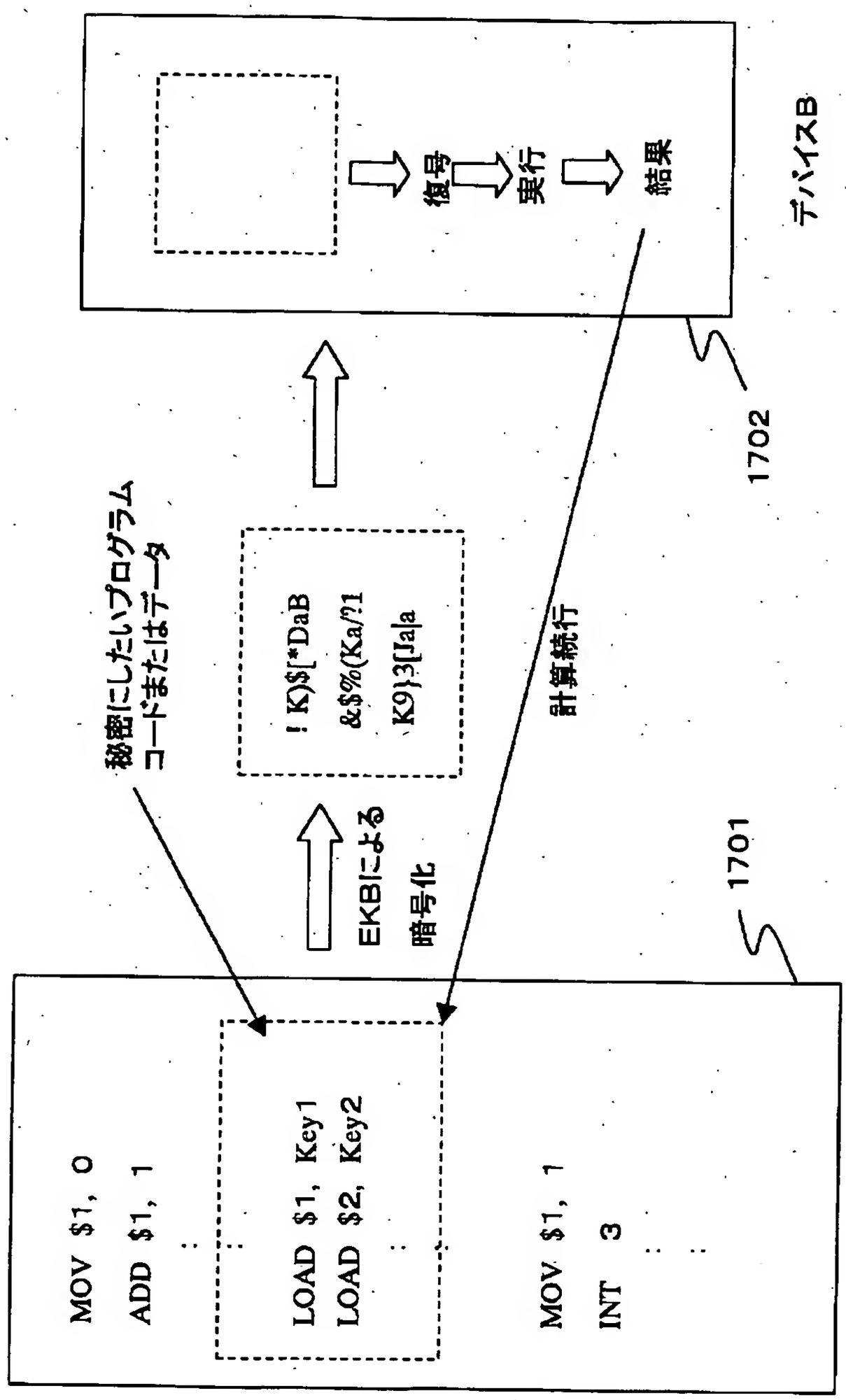
【図15】

ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

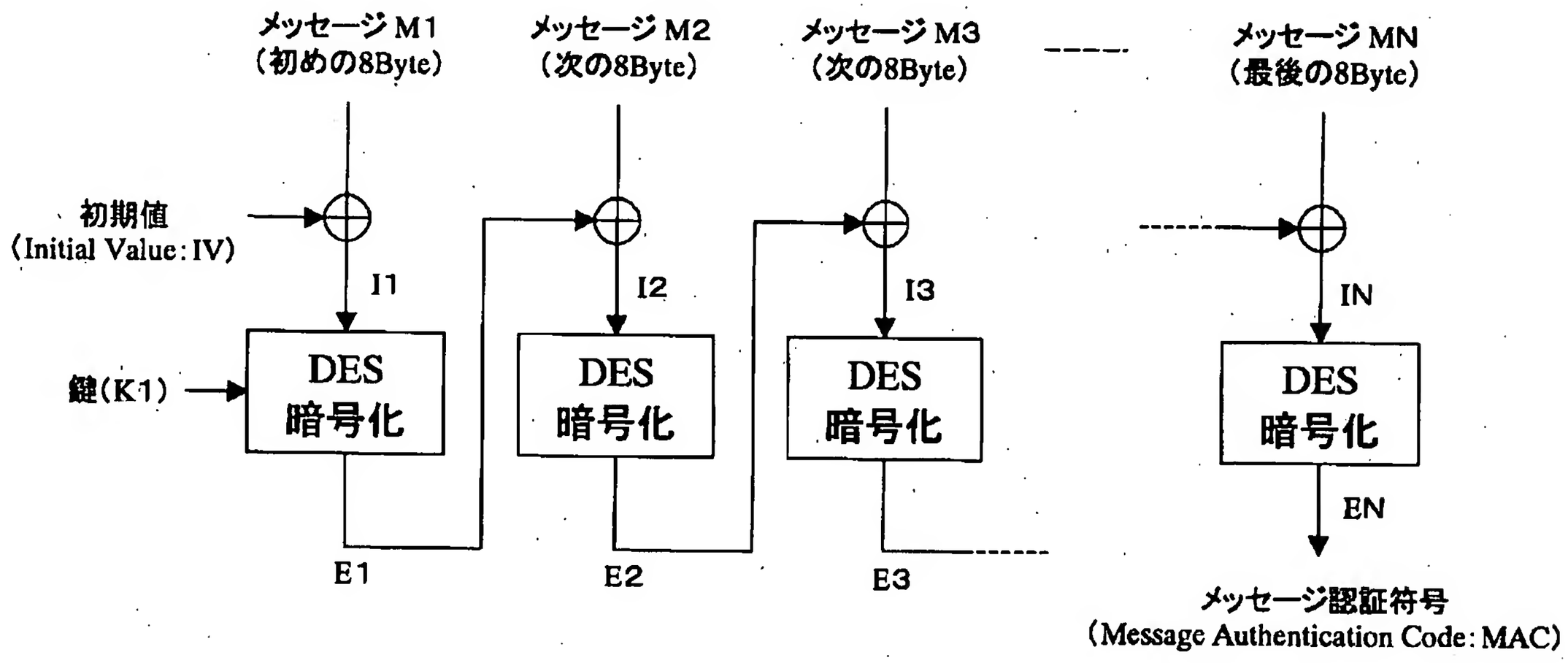

コンテンツ
プロバイダ
AKE
PC
再生
装置
記録
媒体
Kcon
E(Kcon)
+
EKB
Eroot(Kcon)
+
EKB
Eroot(Kcon)
+
EKB
Eses
Knode
Kleaf
Kcon
Eses
E(Kcon)
+
EKB
Eses
Eroot(Kcon)
+
EKB

【図16】

【図１７】

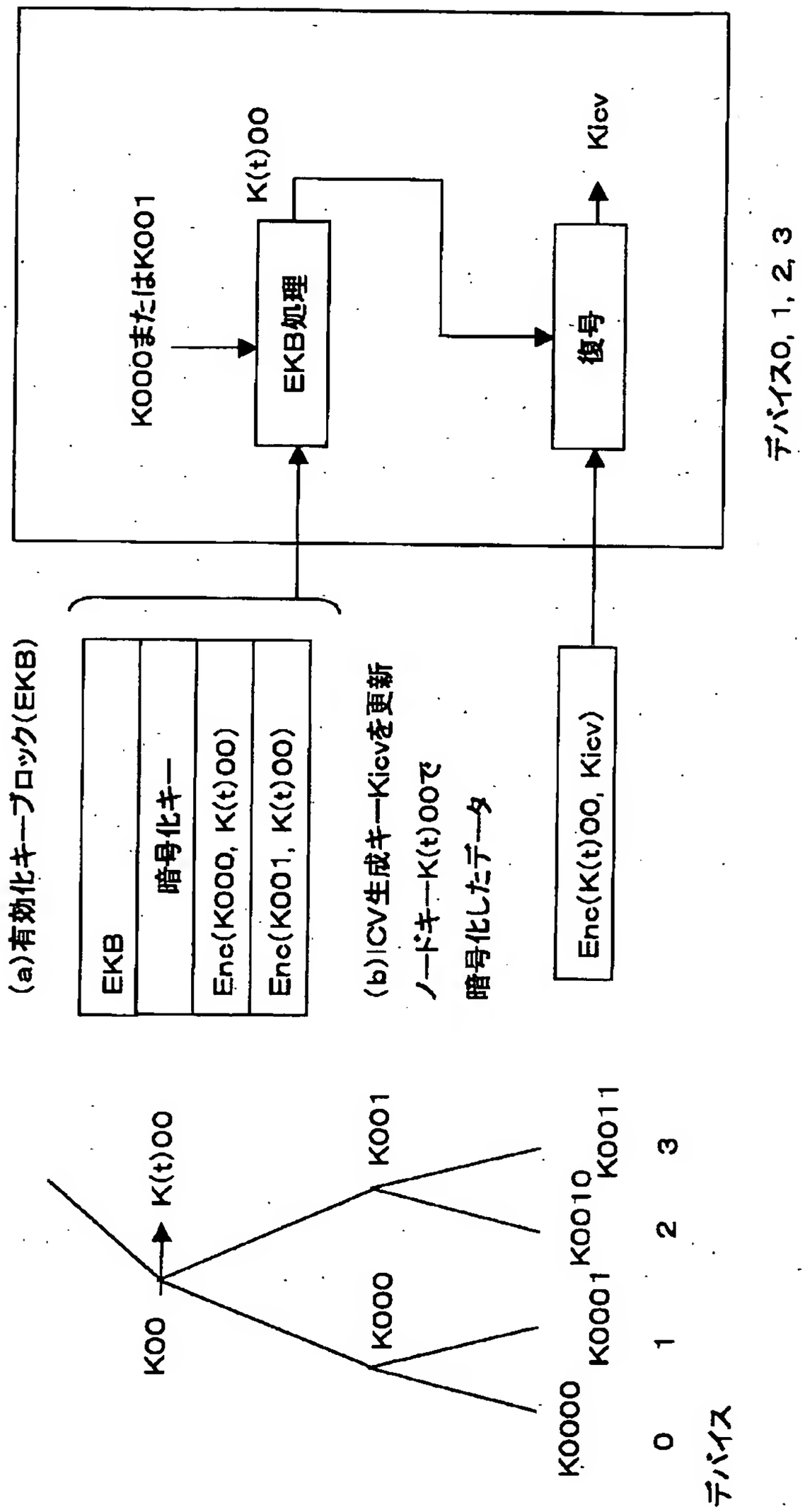

デバイスB
1702
結果
実行
復号
計算続行
秘密にしたいプログラム
コードまたはデータ
! K)$['DaB
&$%(Ka/?1
K9}3[Ja|a
EKBによる
暗号化
1701
デバイスA
MOV $1, 0
ADD $1, 1
LOAD $1, Key1
LOAD $2, Key2
MOV $1, 1
INT 3

【図18】

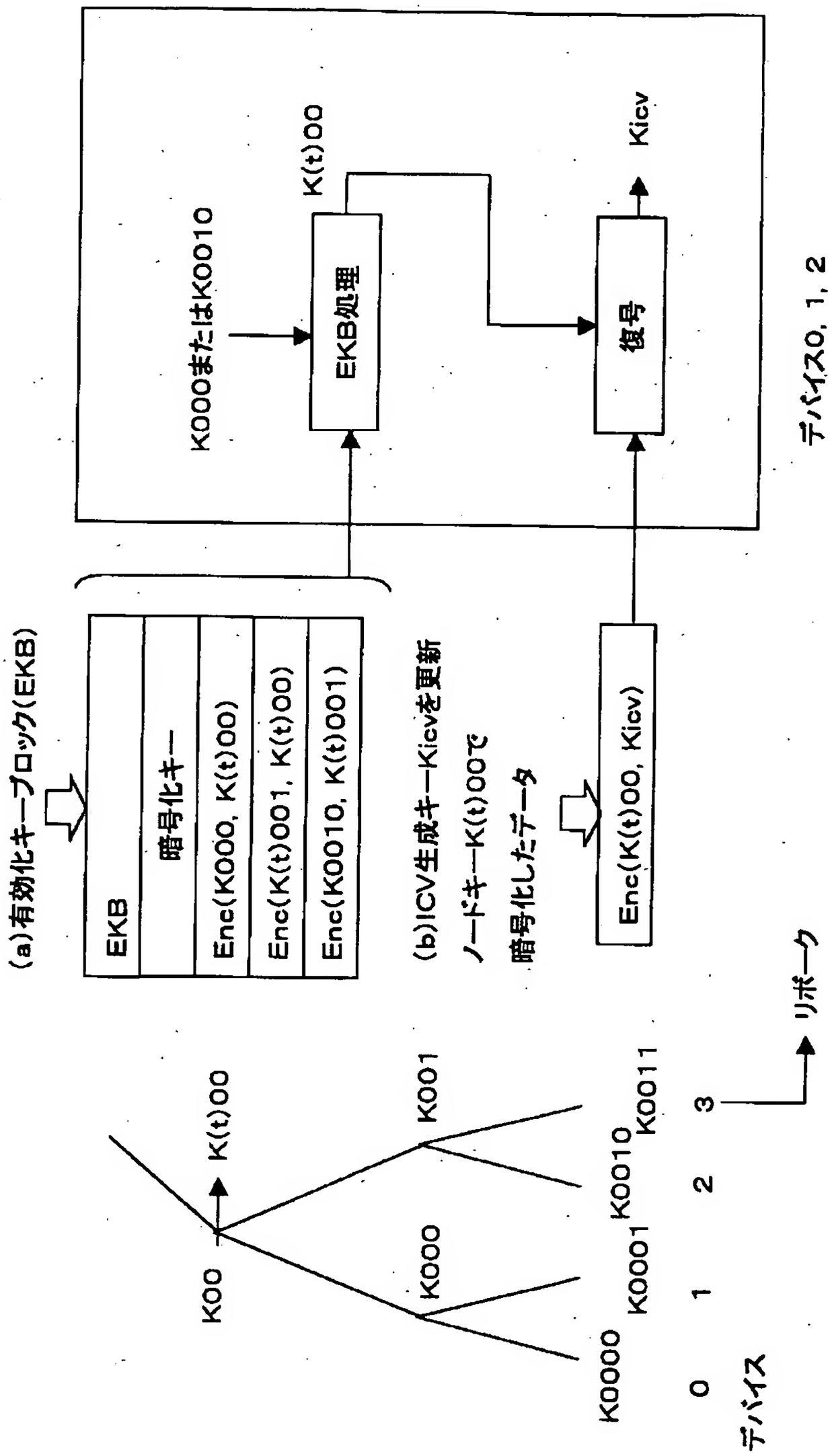


⊕ ：排他的論理和処理（8バイト単位）

【図１９】


K000またはK001
K(t)00
EKB処理
Kicv
復号
デバイス0, 1, 2, 3
(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K001, K(t)00)
(b)ICV生成キーKicvを更新
ノードキーK(t)00で
暗号化したデータ
Enc(K(t)00, Kicv)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
デバイス

【図２０】



フロントページの続き

(72)発明者　大石　丈於
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　光澤　敦
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA07 BA07 CA09
5J104 AA01 AA12 AA16 EA02 EA07
EA17 NA03 NA27 PA07 PA10
PA14